IIR

Internet
Infrastructure
Review

Dec.2017
Vol. 37

Periodic Observation Report

Internet Trends as Seen from IIJ Infrastructure

Focused Research (1)

VSS Does Not Protect User Data

Focused Research (2)

The Commercialization and Economic Sphere of Video Over IP Technology

Focused Research (3)

Intent-Based Network Security

IIJ
Internet Initiative Japan

Internet Infrastructure Review

December 2017 Vol.37

Executive Summary

As announced in the previous volume, we have revised the content of our IIR, and Vol.37 is the second report since this revision. The summary of Internet security, which we published periodically until Vol.35, IIJ's SOC team will now be issuing a monthly observation report from a website called, wizSafe Security Signal. Data from September has been published, and we will endeavor to provide information there in a timely manner, so we encourage you to take a look.

IIJ aims to introduce the wide range of technology that we research and develop in this IIR, which is comprised of periodic observation reports that provide an outline of various data we obtain through the daily operation of services, as well as focused research where we examine specific areas of technology.

Chapter 1 is the periodic observation report for this volume. Here, we examine the state of the Internet, including BGP routes, DNS queries, IPv6 traffic, and mobile traffic, based on information obtained through the operation of IIJ's network and server infrastructure. It is the first time we have presented this information in an IIR, and in some areas, we have only been able to provide interim results, but we intend to continue reporting on this topic regularly going forward.

Chapters 2 through 4 are our focused research. In Chapter 2, we covered VSS (Volume Shadow Copy Service), which is a Windows function related to backups. VSS makes it possible to create snapshots, which can be used to restore the attack tools used by attackers, in addition to temporary and altered files, so they are recognized by analysts as one of the most important pieces of data in digital forensics. However, while performing technical analysis of digital forensic data, we confirmed an issue where user data is not saved correctly to snapshots even when VSS is enabled. We investigated the cause of this issue and the scope of its impact, while also discussing methods for handling it.

Chapter 3 is about video over IP technology, which is quickly garnering interest at broadcasters. Together with the proliferation of the Internet, a variety of media has come to use IP (Internet Protocol) as infrastructure. Magazines and newspapers, as well as music and video content that were once distributed on CDs and DVDs, are now delivered over IP. Currently, one hot topic is the delivery of uncompressed audio and video signals such as those utilized by broadcasters over IP networks. In this chapter, we discuss the reasons why video over IP is necessary, in addition to the status of standardization. We also report on the PoC (Proof of Concept) activities carried out by IIJ.

In Chapter 4, we examine intent-based networking (IBN), which is said to be the next big thing after SDN and SD-WAN. Using IBN, users set the policies they want to implement for their work, and the network verifies the feasibility of these before implementing them automatically. The network also constantly monitors itself and optimizes operation. With IBN, IIJ aims to realize a new system for security that assumes a zero trust environment. In this chapter, we provide concrete details about this initiative, and discuss its future prospects.

IIJ continues to strive towards improving and developing our services daily, while maintaining the stability of the ICT environment. We will keep providing a variety of services and solutions that our customers can take full advantage of as infrastructure for their corporate activities.

Junichi Shimagami
Mr. Shimagami is a Senior Executive Officer and the CTO of IIJ. His interest in the Internet led to him joining IIJ in September 1996. After engaging in the design and construction of the A-Bone Asia region network spearheaded by IIJ, as well as IIJ's backbone network, he was put in charge of IIJ network services. Since 2015, he has been responsible for network, cloud, and security technology across the board as CTO. In April 2017, he became chairman of the Telecom Services Association of Japan MVNO Council.

Internet Trends as Seen from IIJ Infrastructure

IIJ provides Internet services by operating some of the largest network and server infrastructure in Japan. Here, we examine and discuss current Internet trends based on information obtained by operating this infrastructure.

We cover the topics of network routing information and DNS query information, as well as the usage status of IPv6 and mobile access services. We also report on the current state of the backbone network that supports the bulk of IIJ's traffic.

Topic 1

BGP/Number-of-Routes

Six and a half years have passed since February 3, 2011, when the pool of IPv4 addresses was exhausted at IANA, which oversee the allocation of global IP address resources. Currently, all five of the global RIRs (Regional Internet Registries) allocated IP addresses by IANA to allocate to individual countries have begun (or have already finished) the allocation or assignment of addresses from their last /8 block. Meanwhile, the number of IPv4 "full routes" observed on the Internet has been climbing steadily even after the exhaustion of IANA addresses, and is now close to double the amount as it was in 2011. In this section, we once again confirm trends in the number of routes based on IPv4 full-route equivalent information advertised from our network to other organizations (Table 1, Figure 1).

In general, the growth rate tends to be higher for longer prefix routes, which is what we expect. The notable increase in /22 routes is probably due to the size of IPv4 address space allocated/assigned by RIRs whose /8 block is almost depleted being limited to a maximum of /22 (1024 addresses).

Table 1: Trends in the Number of IPv4 Routes for Each Prefix Length Included in Full Routes

	/8	/9	/10	/11	/12	/13	/14	/15	/16	/17	/18	/19	/20	/21	/22	/23	/24	total
September 2010	20	10	25	67	198	409	718	1308	11225	5389	9225	18532	23267	23380	30451	29811	170701	324736
September 2011	19	12	27	81	233	457	794	1407	11909	5907	9885	19515	26476	26588	35515	34061	190276	363162
September 2012	19	14	29	84	236	471	838	1526	12334	6349	10710	20927	30049	31793	42007	39517	219343	416246
September 2013	16	11	30	93	250	480	903	1613	12748	6652	10971	22588	32202	34900	48915	42440	244822	459634
September 2014	16	12	30	90	261	500	983	1702	13009	7013	11659	24527	35175	37560	54065	47372	268660	502634
September 2015	18	13	36	96	261	500	999	1731	12863	7190	12317	25485	35904	38572	60900	52904	301381	551170
September 2016	16	13	36	101	267	515	1050	1767	13106	7782	12917	25229	38459	40066	67270	58965	335884	603443
September 2017	15	13	36	104	284	552	1047	1861	13391	7619	13385	24672	38704	41630	78779	64549	367474	654115
Growth Rate*	0.75	1.3	1.44	1.552	1.434	1.35	1.458	1.423	1.193	1.414	1.451	1.331	1.663	1.781	2.587	2.165	2.153	2.014

*September 2017 values with September 2010 value normalized to 1

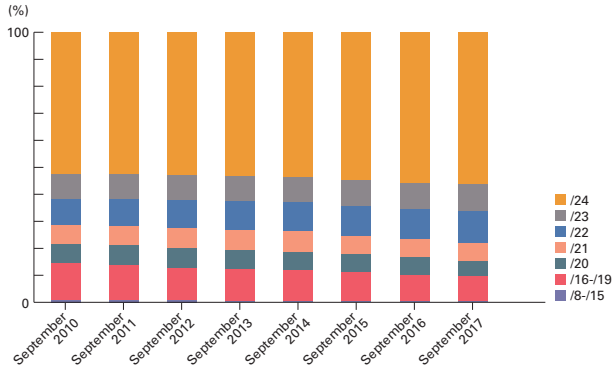

Figure 1: Trends in the Number of Routes for Each Prefix Length as a Proportion of IPv4 Full Routes

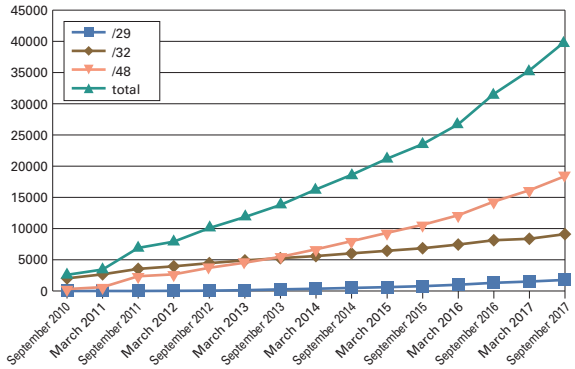

Figure 2: Trends in the Number of IPv6 Full Routes

You can also see that while the number of /8 routes is decreasing, all the others are increasing. We believe this is caused by the splitting of address blocks for the purpose of address transfers. Put simply, when an address block is split, the number of routes on the left side of Table 1 decreases, while the number of routes on the right side increases. It is likely that address transfers will continue to be used as a valuable means of obtaining IPv4 addresses, so we expect the distribution of the number of IPv4 routes to become even more biased toward the right side of Table 1 (with the longer prefixes).

In closing, we will touch upon the number of full routes for IPv6, the successor to IPv4 (Figure 2). Although the number is still insignificant compared to IPv4, it is increasing steadily, and from around 2016 this trend seems to have gained momentum. With the supply of IPv4 addresses from each RIR becoming further depleted, we speculate that support for IPv6 on a regional and organizational level will accelerate in the future. It will be interesting to see how this trend changes going forward.

Topic 2

DNS

IIJ provides a full resolver to enable users of our Internet access services to use DNS name resolution. In this section, we discuss the state of name resolution, and analyze and reflect upon data for servers mainly provided for broadband, based on a day's worth of full resolver observation data obtained by IIJ on May 17, 2017.

Full resolvers only know the IP address of the authoritative name server that provides top-level zone information, which is known as the root. Based on the information gained from there, they track down authoritative name servers likely to possess information for locating the required record. Because load and latency become an issue when making recursive queries each time using a full resolver, the records obtained are cached for a while, and retrieved from the cache when the same query is received again. Recently, functions related to DNS have also begun to be implemented in devices on the communication route, such as broadband routers or firewalls. These may be involved in relaying DNS queries or applying control policies.

On broadband and mobile connections, it is possible to use protocols such as PPP, DHCP, RA, and PCO to notify users of the IP address of the full resolver. ISPs use these functions to enable automatic configuration of full resolvers for the name resolution required by user communications. ISPs can inform users about multiple full resolvers, and users can specify and add full resolvers to use by changing settings themselves. When more than one full resolver is configured on a computer, the one used depends on the computer's implementation or application, so full resolvers are not aware of the total number of queries being sent by a user. This means that full resolvers must be operated with extra processing power in reserve, while keeping a close watch on query trends.

Looking at user trends in the observation data for the full resolver provided by IIJ, we observe a daily average of about 0.08 queries/sec per source IP address. This value fluctuates depending on the time of day, indicating trends in user activity, with about 0.04 queries/sec at around 4:00 a.m., and about 0.13 queries/sec during the peak at around 9:00 p.m. Both the IPv6 and IPv4 IP protocols are used for query communications, and these exhibit almost identical trends, with queries via IPv6 showing slightly greater variance due to the time of day. These values have not undergone any significant change over the past few years, staying within a variation range of about 0.06 points. Variable elements include the number of full resolvers that can be used by a client, the caching function in the user environment, and the behavior of computers and applications. This means it is hard to anticipate future trends, making continuous observation necessary.

Looking at the query record types, most are A records that query the IPv4 address corresponding to the host name, and AAAA records that query IPv6 addresses. There are differences in trends between the IP protocols used for query communications, with more AAAA record queries seen for IPv6 queries. For IPv4 queries, about 64% of the total are A record queries, while about 33% are AAAA record queries (Figure 3). Meanwhile, about 56% of total IPv6 queries are A record queries, and a higher ratio of about 43% are AAAA record queries (Figure 4). Also, examining trends for each query source IP address, about 96% are attempts to search for A records, regardless of whether the query was made via IPv4 or IPv6. As for AAAA records, about 57% of query sources in IPv4 and about 80% in IPv6 are searches. The ratio of records that account for IPv4 queries has not changed a lot in the past few years, so we surmise that new implementations in recent years may prioritize using IPv6 for queries.

Topic 3

IPv6

On February 3, 2011, the IPv4 address pool of the APNIC RIR that manages IP address resources in the Asia-Pacific region was exhausted, and the new allocation of regular IPv4 addresses (assignment to regional management organizations and ISPs) ended in Japan. In other words, the stock of IPv4 addresses was depleted. About six and a half years have passed since then, but it still cannot be said that there has been an explosive spread in the use of its successor, IPv6.

Here, we will analyze IPv6 user numbers, traffic and usage protocols at IIJ and explain their current state.

■ Number of Users

IIJ started offering IPv6 PPPoE connections to customers using the FLET'S HIKARI NEXT service of NTT East and NTT West in June 2011. From July 2011, we also began providing IPv6 IPoE connections (in collaboration with affiliate INTERNET MULTIFEED CO.). In July 2015, we launched support for IPv6 PPPoE automatic connection from home gateways rented out by NTT East/West, so that customers can use IPv6 connection without special settings. On our mobile services, we also provided support for IPv6 connections since the launch of our 4G (LTE) plans in May 2012. This enables mobile IPv6 connections as long as the device supports IPv6.

Figure 5 shows trends in the number of IPv4 and IPv6 connections on FLET'S HIKARI NEXT from July 2015 to the end of September 2017. IPv4 saw a negligible decrease, while IPv6 increased slightly, and as of September 2017 IPv6 accounts for approximately 22.9% of total connections (PPPoE 22%, IPoE 0.9%).

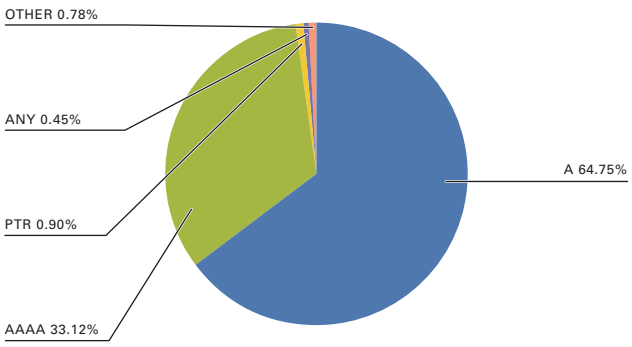

Figure 3: IPv4-based Queries From Clients

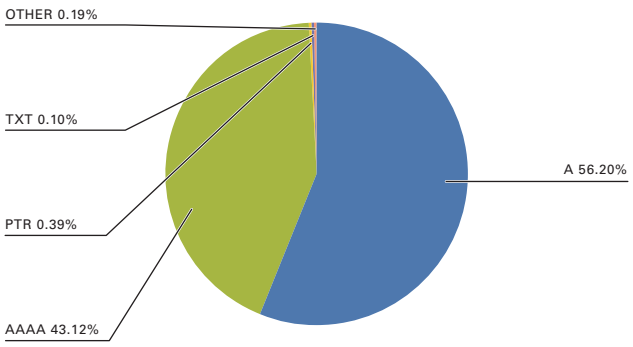

Figure 4: IPv6-based Queries From Clients

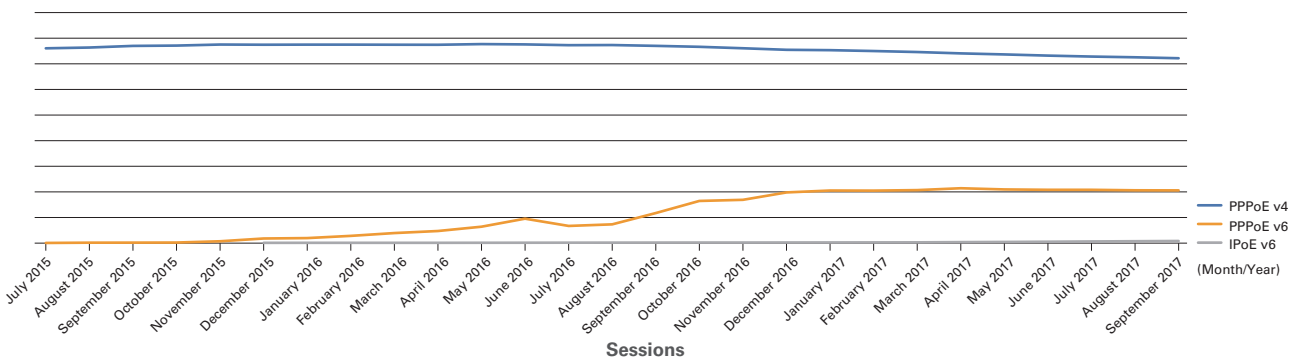

Figure 5: Trends in the Number of IPv4 and IPv6 Connections on FLET'S HIKARI NEXT from July 2015 to the End of September 2017

We believe that the number of IPv6 users has remained at around 22.9% because some users have devices that do not support IPv6 PPPoE automatic connections, and others have signed corporate contracts that do not provide IPv6, so we do not foresee there being any big increases in IPv6 PPPoE from here on. While IPv6 IPoE numbers are still low right now, we expect that migration to IPv6 IPoE using DS-Lite will gradually progress, and the gap will shrink.

Traffic

Figure 6 shows IPv4 and IPv6 traffic measured using IIJ backbone routers at core POPs (points of presence – in Tokyo, Osaka, and Nagoya). Both IPv4 and IPv6 are climbing, but IPv6 traffic only accounts for about 4% of the total. As a result, it is overshadowed by the IPv4 results when the two are put alongside, so at the moment it is difficult to say that it is gaining in popularity.

Next, Figure 7 shows the top annual average IPv6 traffic source organizations (BGP AS number) from October 2016 to September 2017.

At the top of the rankings is Company A, which is actively moving ahead with IPv6 support on its services, with the companies second and lower reaching just 1/16 of its numbers.

Company A also leads the IPv4 rankings (Figure 8), followed by major cloud vendor Company D in second, then major CDNs Company G and Company K. It is interesting to see the difference in types of organizations compared to IPv6. Another difference is that the number two company is at about 1/2 the level of Company A in the lead, unlike the differences for IPv6.

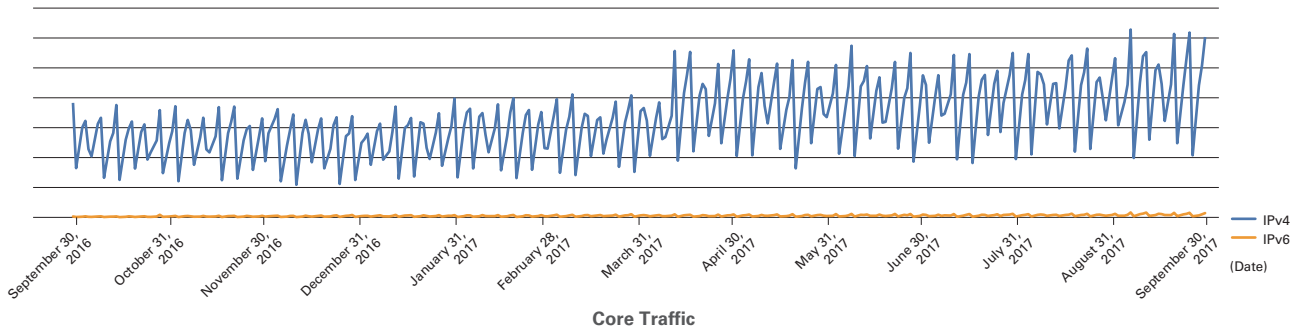

Figure 6: IPv4/IPv6 Traffic Measured Via IIJ Backbone Routers at Core Population Centers (Tokyo, Osaka, and Nagoya).

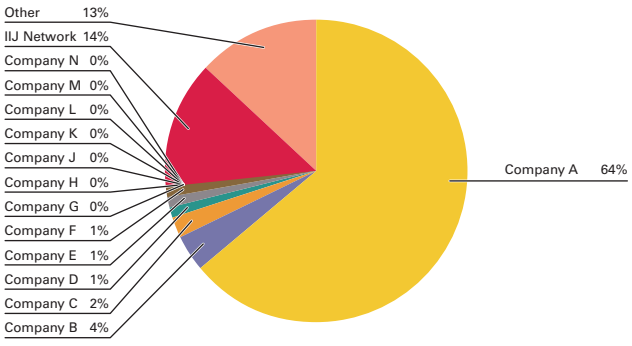

Figure 7: Top Annual Average IPv6 Traffic Source Organizations (BGP AS Number) from October 2016 to September 2017

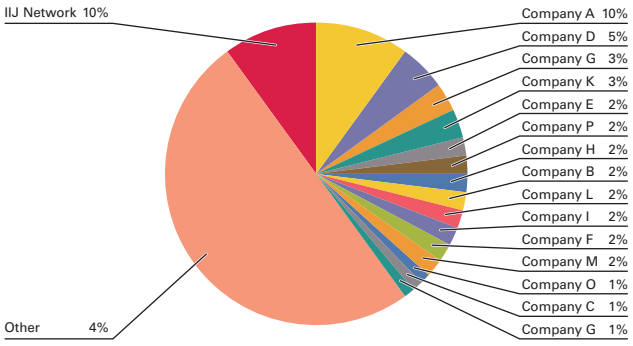

Figure 8: Top Annual Average IPv4 Traffic Source Organizations (BGP AS Number) from October 2016 to September 2017

Looking at the gap in traffic volume between Company A and those below, we would hazard a guess that although business operators other than Company A provide services with IPv6, its use may be limited.

Protocols Used

Figure 9 shows a graph analyzing via the protocol number (Next-Header) and source port number of IPv6 traffic (for a one-week period from October 1, 2017).

443/TCP (HTTPS) accounts for about 40% of the total, rising to over 50% when combined with 443/UDP (which we believe is QUIC) in second. Although 80/TCP (HTTP) is in third, this amounts to only about 1/6 of second and first combined, showing a difference that is quite remarkable compared with the IPv4 graph for the same period (Figure 10). We believe that IPv6 has a higher ratio of HTTPS/QUIC because Company A accounts for a large proportion of traffic. However, this may also be explained by new services from other companies that support IPv6 also being provided via HTTPS since its launch.

Summary

In this report we examined user numbers, traffic volumes, and usage protocols for the current state of IPv6 at IIJ. Although the environment for IPv6 connections has improved, the impression we get is that, aside from one company, support is only just beginning from the service provider side. With the three major Japanese carriers (NTT DOCOMO, KDDI, and SoftBank) having announced support for IPv6 one after another in 2017, we expect that support by service providers will gain momentum going forward. We will continue to analyze the situation from a variety of perspectives.

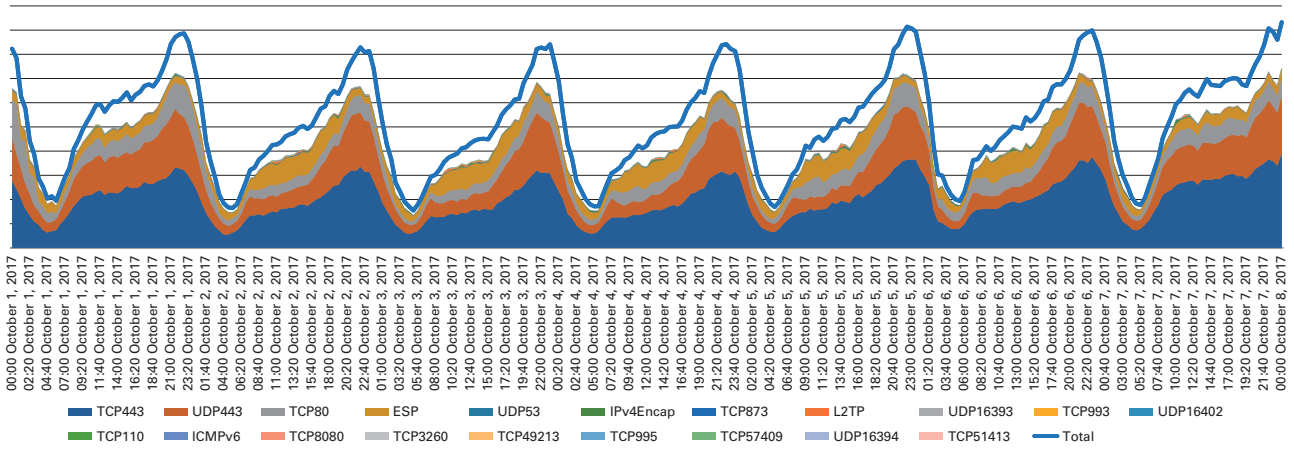

Figure 9: Graph Analyzing via Protocol Numbers (Next-Header) and Source Port Numbers of IPv6 Traffic

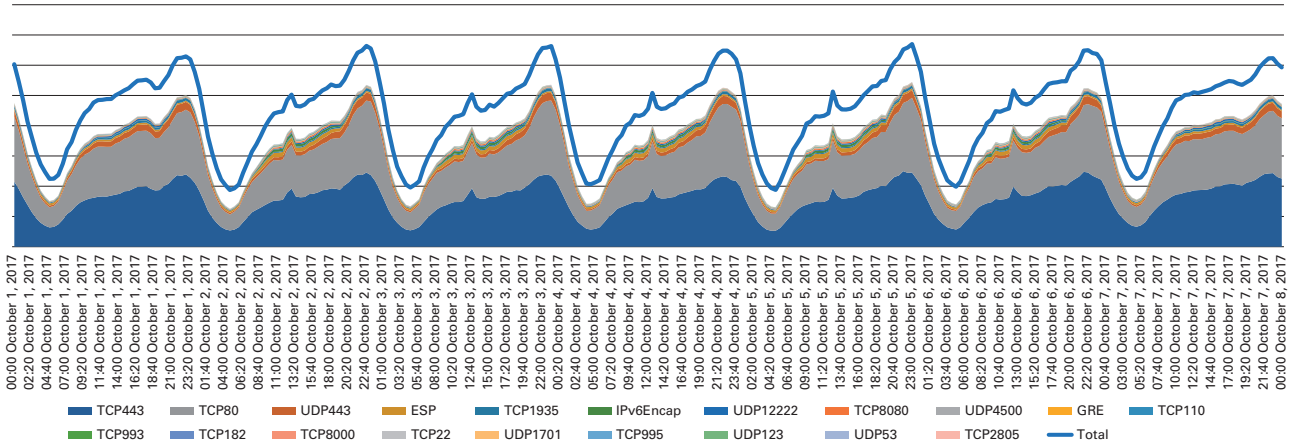

Figure 10: Graph Analyzing via Protocol Numbers and Source Port Numbers of IPv4 Traffic

Topic 4

Mobile

In this report, we analyze mobile traffic trends by focusing on time of day.

Figure 11 shows trends in traffic (bps) over the course of a single working weekday. The vertical axis represents relative traffic volume, while the graph shows the changing trends. These days, most mobile service users use smartphones. As you can imagine considering the situations where smartphones are used, the three large peaks in the graph correspond to the morning commute to work or school, the midday lunch break, and the commute back home from work or school in the evening. Traffic also drops sharply after 11:30 p.m.

We can see that usage is most concentrated at around 12:00 p.m. This is because, although the commute times to and from work and school in the morning and evening are spread out, lunch breaks are closely packed together around 12 o'clock. This causes congestion during this time of day. The TCP/IP mechanism controls traffic when congestion occurs, but despite this traffic levels remain high. To raise the utilization rate of facilities, it is important for ISPs to level out traffic variance at different times of the day by creating demand in areas other than smartphones, but this is not an easy task.

Figure 12 is a graph showing the traffic for a given week. You can see a similar pattern repeating from Monday to Friday. While the lunchtime peak at 12:00 p.m. is smaller on Saturday and Sunday, there is no decline in traffic during the day. The dip between Sunday night and Monday morning is also deeper. Although it is hard to see on this graph, the dip in traffic at night tends to become shallower over the weekend. This is an interesting trend that reflects our day-to-day activities.

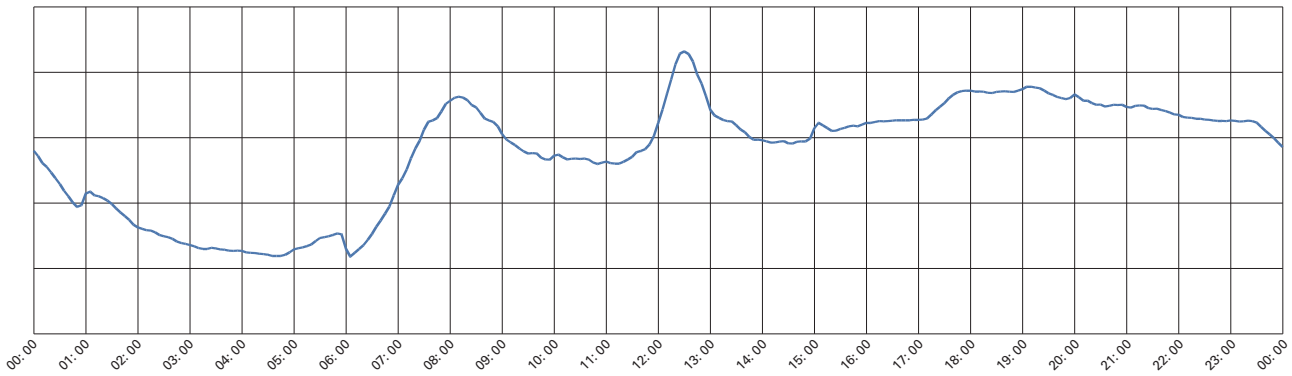

Figure 11: Download Traffic Trends for One Day

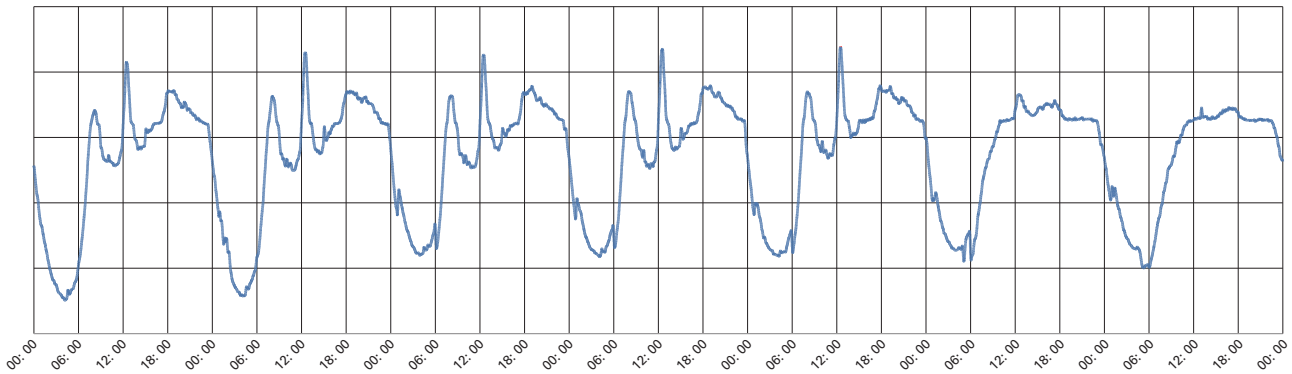

Figure 12: Download Traffic Trends for One Week

Figure 13 plots the daily data transfer volume calculated from the traffic graph for each day. This graph shows data for October, but almost identical trends can be seen in other months when there are no large consecutive holidays, such as the year-end and New Year holidays. Transfer volumes are small at the start of the week, but increase the closer you get to Friday, then decrease over the weekend. Transfer volumes may climb as the weekend approaches because more and more data is transferred at night. It is also thought that the transfer volumes go down on the weekend because data transfers are offloaded to broadband-connected devices in the home. Interestingly, transfer volumes also go down towards the end of the month. We think this is because communications are reduced for users who have used up their monthly data allowance, but we have not yet found evidence to support this. At the start of a new month, transfer volumes that had been low at the end of the previous month will recover to their original levels or higher. Looking at overall mobile traffic throughout the year, we can see it is increasing steadily.

For some people, smartphones are essential items closely related to our everyday lives. This can be seen clearly in mobile traffic trends.

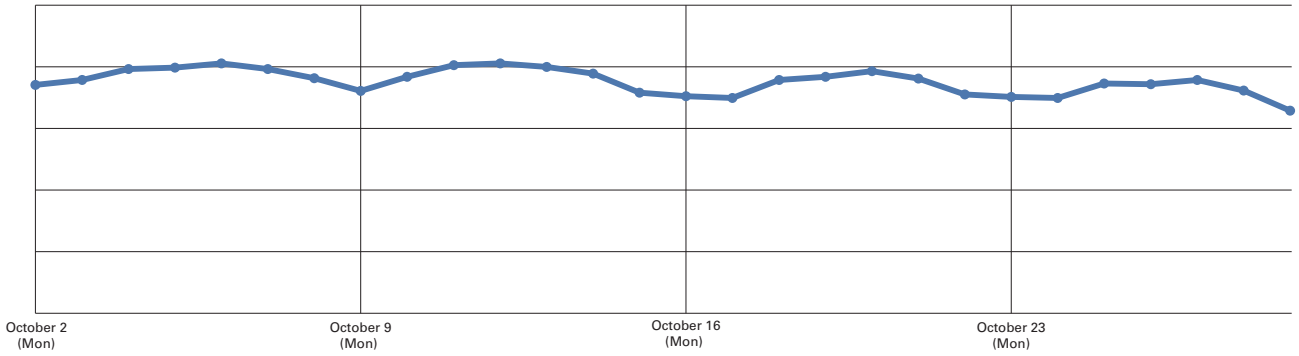

Figure 13: Data Transfer Volume by Date

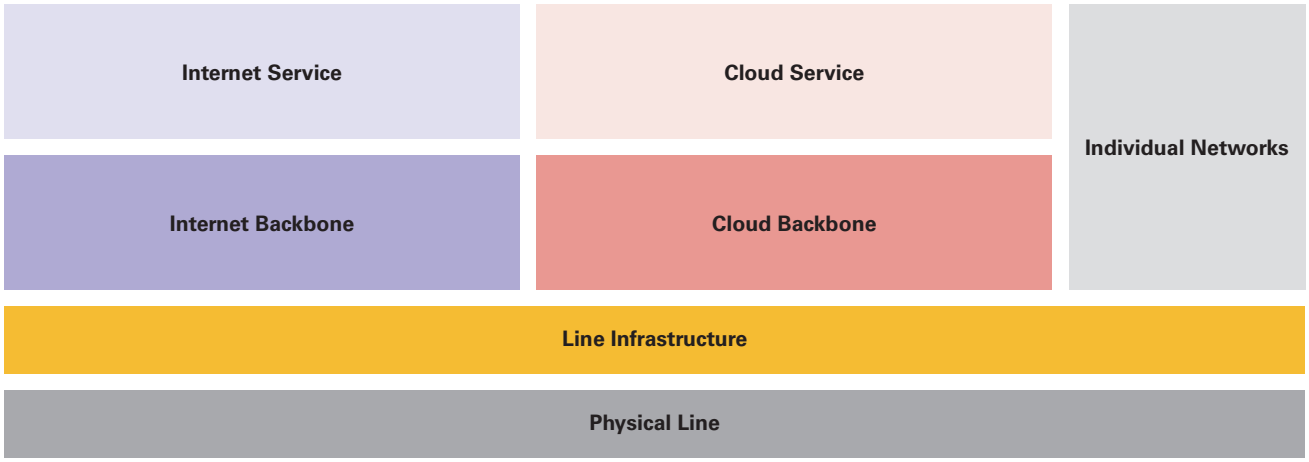

Figure 14: IIJ Backbone Structure

Topic 5

IIJ Infrastructure (Backbone)

Here we give an overview of IIJ backbone infrastructure.

Traffic is increasing at a steady rate. Overall Internet traffic has grown by a factor of 1.35 times per year on average, and the number of access lines in Japan and the U.S. has increased by 1.2 times on average annually (over the past four years in each case). Cloud traffic including services such as IIJGIO has also increased by 2.5 times over the past two and a half years.

Backbone infrastructure has evolved to support this increase in traffic. In terms of scale, we have extended the 100G line implemented between Tokyo, Nagoya, and Osaka three years ago to regional POPs, a connection between Japan and the U.S., and even to locations on the east coast of the U.S. Meanwhile, there have also been structural changes. Current backbone infrastructure establishes a layer 2 closed network (line infrastructure) for providing virtual lines over physical ones, and the backbone for Internet and cloud solutions is configured on the virtual lines provided by this infrastructure. Internet and cloud traffic are both provided over the same physical line, and traffic engineering implemented in the layer 2 closed network improves the efficiency of line utilization and increases the cost benefits. Another significant benefit is that this structural change has also made it possible to freely build networks without being bound by geographical restrictions. You could say the new IIJ DDoS Protection Service launched during the last fiscal year for handling large-scale attacks was made possible by this structural change. We will continue to evolve our backbone infrastructure to provide a variety of network services related to the Internet and cloud computing.

Authors:

1. BGP/Number-of-Routes
Tomohiko Kurahashi
Infrastructure Planning Department, Service Infrastructure Division, IIJ

2. DNS
Yoshinobu Matsuzaki
Infrastructure Planning Department, Service Infrastructure Division, IIJ

3. IPv6
Taisuke Sasaki
Infrastructure Planning Department, Service Infrastructure Division, IIJ

4. Mobile
Takanori Sasai
Mobile Technology Section, Network Technology Department, Service Infrastructure Division, IIJ

5. IIJ Infrastructure (Backbone)
Daisuke Sugawara
Backbone Technology Section, Network Technology Department, Service Infrastructure Division, IIJ

VSS Does Not Protect User Data

2.1 Introduction

VSS, an abbreviation for Volume Shadow Copy Service, is a backup-related function found in Windows XP / Windows Server 2003 and later versions of Windows.

VSS can create snapshots, enabling you to save the state of a volume at a given point in time. Users can access data on a volume from the time a snapshot was created by referencing the snapshot. This includes deleted files and files with data that has been modified. Snapshot data is not updated because it is read-only. Also, files that are locked in a volume are not locked in a snapshot. It is possible to perform a complete backup by taking advantage of such characteristics.

Snapshots are also used for the files that can be restored from the "Previous Versions" tab displayed in the file and folder properties in Windows 7/10 (Figure 1). Many may recall that restoring files from a snapshot was a workaround discussed when Ransomware became prevalent.

Because snapshots can be used to recover attack tools used by attackers in addition to temporary and altered files, they are recognized by analysts as one of the most important pieces of data in digital forensics. However, while performing technical analysis of digital forensic data, we confirmed an issue in Windows 8.1/10 where user data is not saved correctly to snapshots even when VSS is enabled. We investigated the cause of this and the scope of its impact. We also discuss methods for handling this issue here.

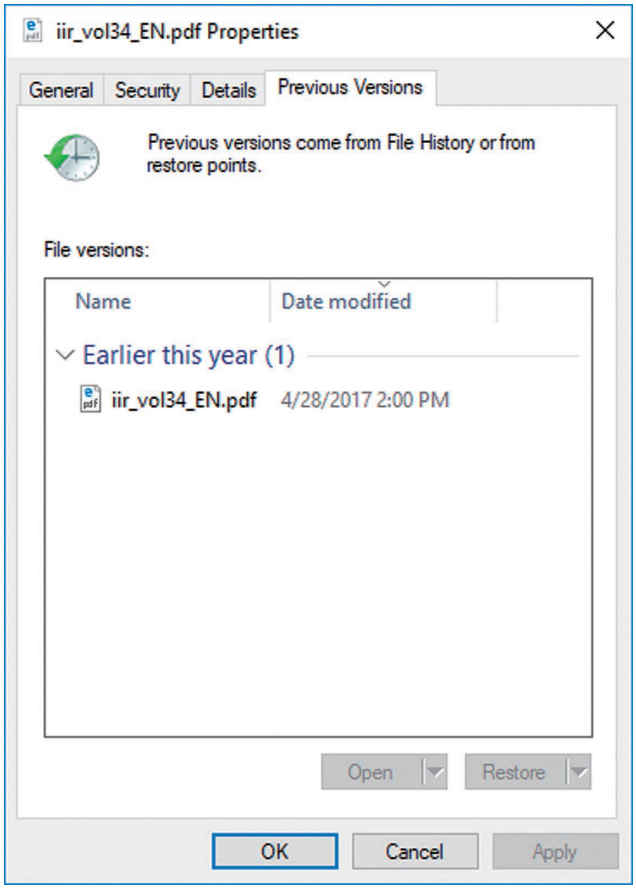

Figure 1: "Previous Versions" Tab

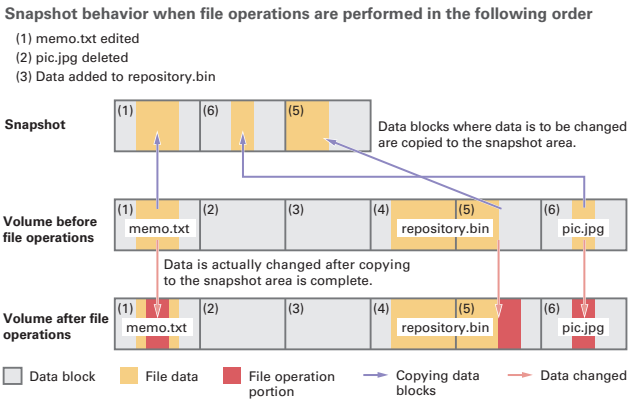

Figure 2: Saving Difference Data

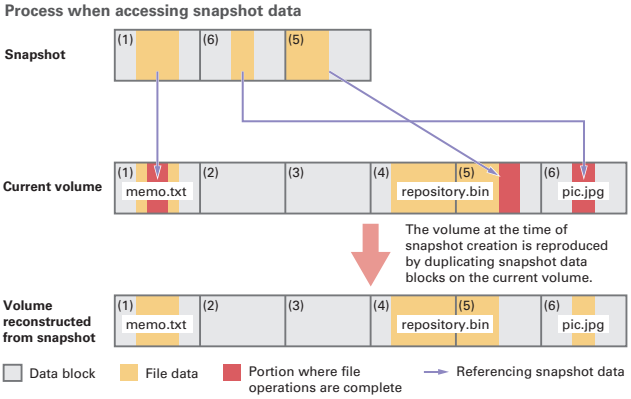

Figure 3: Accessing a Snapshot

2.2 VSS Snapshot Mechanism

As mentioned above, a snapshot saves the state of a volume at any given point in time, but it does not save the data at an individual file level. For example, saving an entire set of files when only 1 MB of a 1 GB total has changed leads to poor utilization of a volume, lowering overall OS performance.

Thus, only difference data is saved to the snapshot. To obtain difference data, the entire volume is split into data blocks of 16 KB each, and data for blocks that were changed after snapshot creation is saved along with the offset (Figure 2). When accessing files in a snapshot, the difference data is transparently integrated with the current volume data, reconstructing the data from when the snapshot was created (Figure 3).

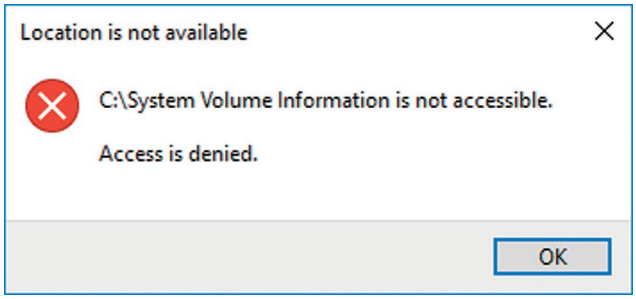

Figure 4: Snapshots Protected from User Access

2.3 VSS Snapshot File Organization

Files related to snapshots are saved to the "System Volume Information" folder directly under the root folder of a volume, but they cannot be accessed using Explorer (Figure 4). In Figure 5, these files are displayed using FTK Imager*1.

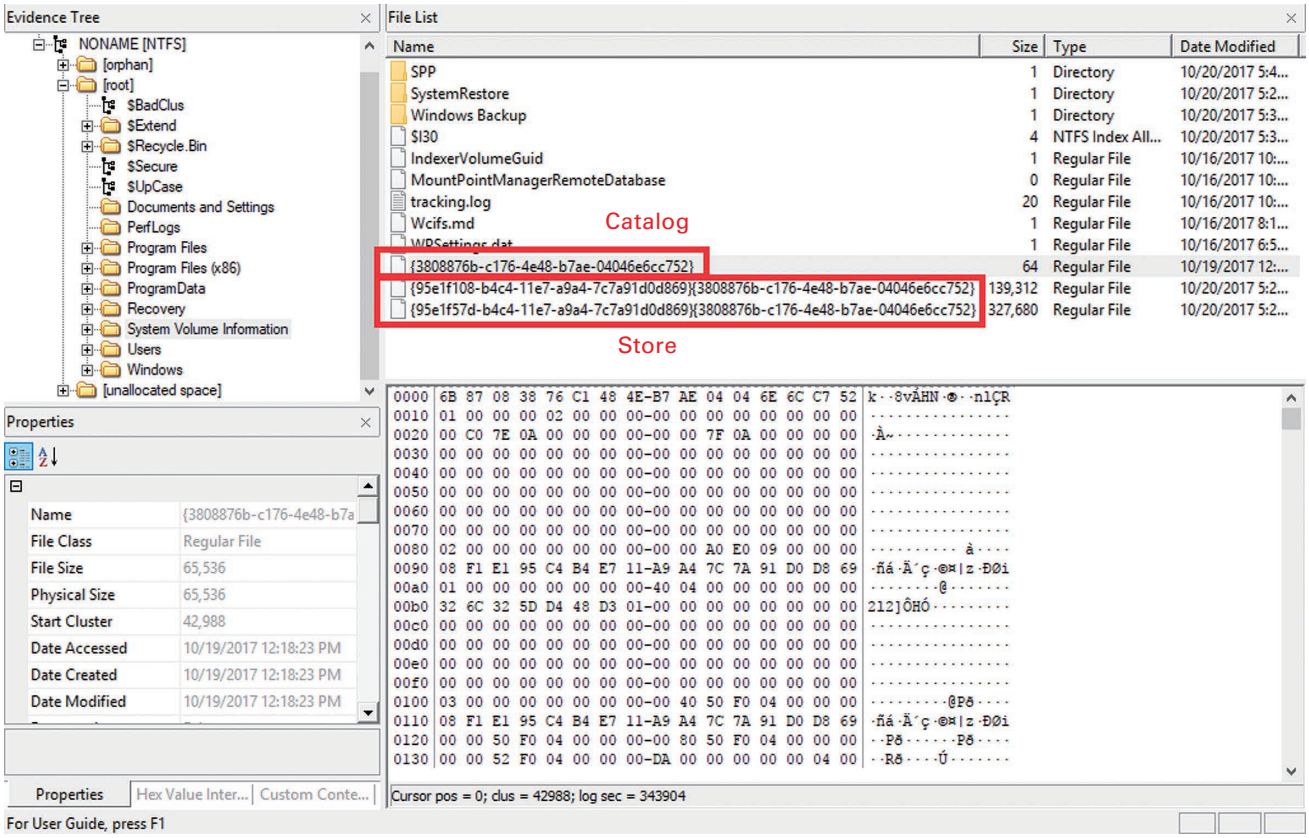

Figure 5: File Organization in the "System Volume Information" Folder

*1 FTK Imager (https://accessdata.com/product-download).

Snapshots consist of two file types: “catalog” and “store” files. Catalog files have “{Catalog GUID}” as their file name, and contain metadata such as the day the snapshot was created and the store GUID. Store files contain the actual data, and have the file name “{Store GUID}{Catalog GUID}*2.”

2.4 Enabling VSS and Snapshot Operations

You can check whether VSS is enabled in “System Properties” (Figure 6). If it is disabled, click the “Configure” button to display the “System Protection for Local Disk” dialog box. Select “Turn on system protection,” set the “Disk Space Usage,” and then click the “OK” button (Figure 7). To create a snapshot manually, click the “Create” button in Figure 6.

It is possible to create multiple snapshots within the same volume, but the oldest snapshot will be deleted when the “Disk Space Usage” configured in Figure 7 is exceeded.

You can view a list of created snapshots and delete them using vssadmin.exe. Open the Command Prompt as an administrator and execute “vssadmin.exe list shadows” to obtain a list of snapshots (Figure 8). It is also possible to perform snapshot operations from WMI and PowerShell.

2.5 File Recovery Tests

We tested the recovery of files saved to a snapshot to verify whether files created by a user are saved correctly to the snapshot. As test user data, we saved the ten PDF files for IIR Vol.26 to Vol.35, which are available on our website, in a folder named “PDF” on the desktop, and then created a snapshot.

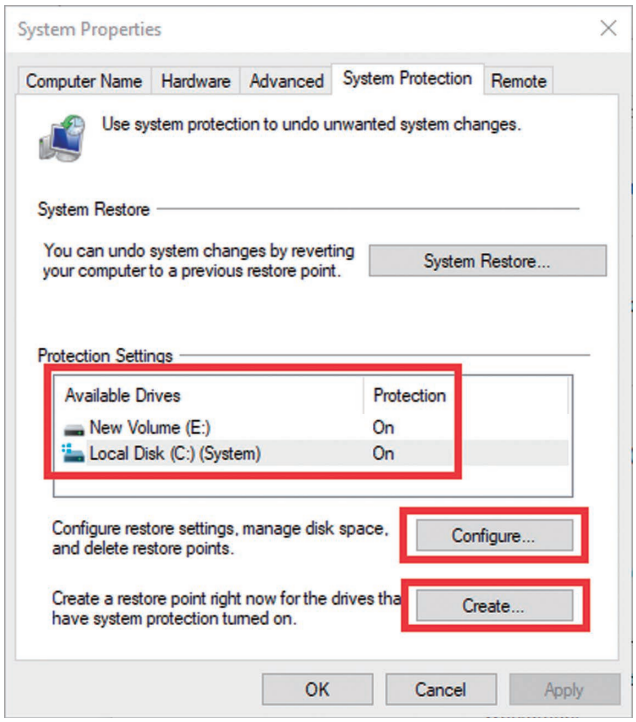

Figure 6: “System Properties” Dialog Box

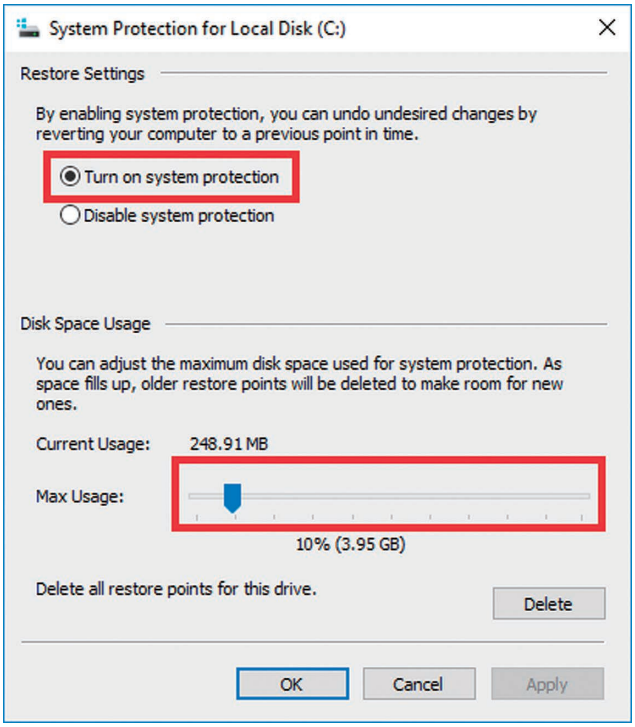

Figure 7: “System Protection for Local Disk” Dialog Box

*2 We do not address the file or data structure of snapshots here. For more information, Volume Shadow Snapshot (VSS) (https://github.com/libyal/libvshadow/blob/master/documentation/Volume%20Shadow%20Snapshot%20(VSS)%20format.asciidoc) is a very useful reference document.

We used the SDelete*3 file deletion tool to delete the files in the "PDF" folder, and then recovered the data from the snapshot using ShadowExplorer*4.

We performed these tasks in Windows 7 SP1 and Windows 10 1703 environments, and listed the MD5 hash values*5 of each PDF file recovered from the snapshot in Table 1. Although we were able to successfully recover all files in Windows 7, all files were corrupted in Windows 10.

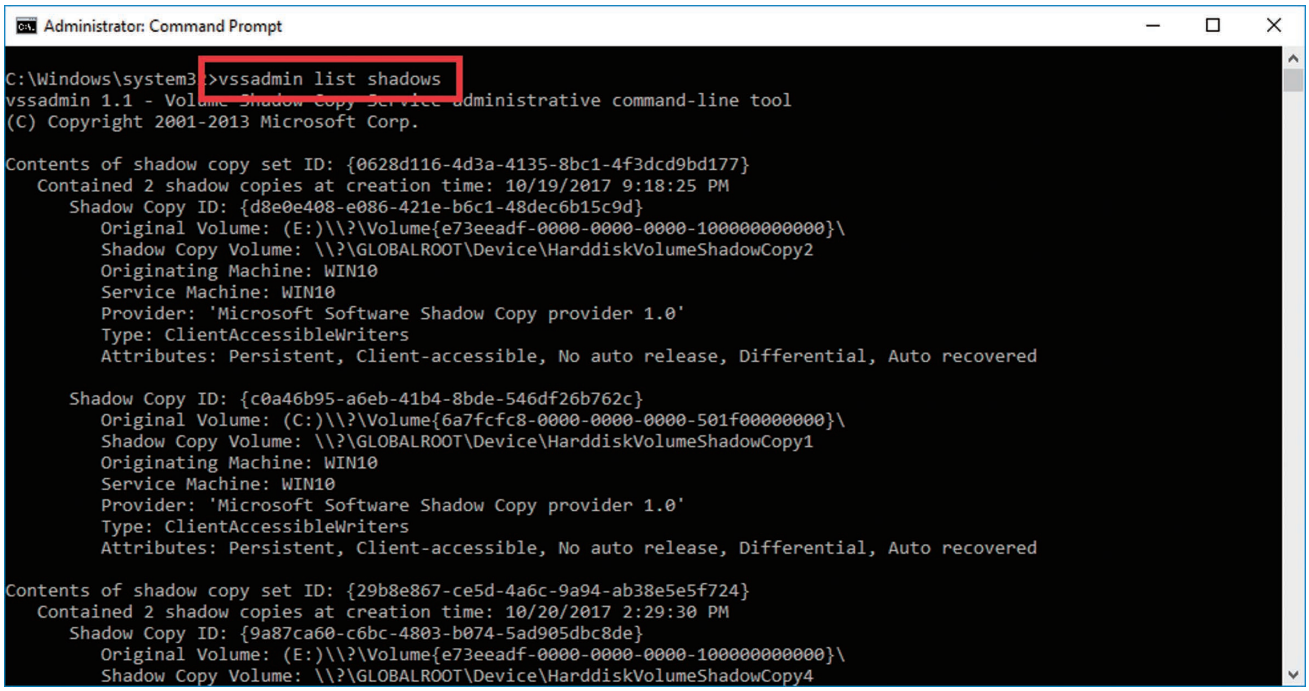

Figure 8: Snapshot List

File name	MD5 of original file	Windows 7 SP1		Windows 10 1703	
		MD5 of recovered file	Match	MD5 of recovered file	Match
iir_vol26_EN.pdf	a3002c631ca894034b594ec4e1a7c285	a3002c631ca894034b594ec4e1a7c285	Yes	42b4ac3f7e2f349ed8a0d3e240db35a6	No
iir_vol27_EN.pdf	09339fc3375988f8f769ccfa7ac75d4f	09339fc3375988f8f769ccfa7ac75d4f	Yes	e4986e8866435b7273f16a7f8fe60a14	No
iir_vol28_EN.pdf	89fee5ffccfb5be9749639e7e65a218e	89fee5ffccfb5be9749639e7e65a218e	Yes	86ff8c095a5b116e1ff34e12d6999053	No
iir_vol29_EN.pdf	42edeccedd51eecc20d0d9c123329b9a	42edeccedd51eecc20d0d9c123329b9a	Yes	5a8a530c084e5ee8ec129c62afa5ab0e	No
iir_vol30_EN.pdf	25df11281a2b1fb72a3f6d48d697c6b4	25df11281a2b1fb72a3f6d48d697c6b4	Yes	a4a68b122007b80a24ca2457e69b0902	No
iir_vol31_EN.pdf	79eac7926477141397f179654d307473	79eac7926477141397f179654d307473	Yes	b8cac677d7cf6bf15594a477c4b1b104	No
iir_vol32_EN.pdf	a99869ea8ea3cbda032d36ba000cdd26	a99869ea8ea3cbda032d36ba000cdd26	Yes	1bd79719c9c91c52e1de214a16572f90	No
iir_vol33_EN.pdf	a246c3f7ef836a141eb9c181899003f3	a246c3f7ef836a141eb9c181899003f3	Yes	17b820ab7f61a6de25cfcc89a1f49e62	No
iir_vol34_EN.pdf	093f3757b7a9269655d9fa6816b6dc72	093f3757b7a9269655d9fa6816b6dc72	Yes	b3c354a635ec62d747ae20aa71f46ab0	No
iir_vol35_EN.pdf	256dd74e71e1080170ddf59d0757e230	256dd74e71e1080170ddf59d0757e230	Yes	6220ce0b3df16961123438bd524568ce	No

Table 1: Comparison of Recovered Files

*3 SDelete (https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete).
*4 ShadowExplorer.com (http://www.shadowexplorer.com/)
*5 MD5 hashes are known to be prone to collisions, but they were used here to compare the identity of specific files, as well as due to space limitations.

2.6 Cause of File Corruption and Countermeasures

Comparing a corrupted file and normal file using a binary editor, we can see that part of the file has been overwritten with null bytes (0x00) (Figure 9). The original file is shown on the left, while a file recovered using Windows 10 is on the right. The red part is where the data does not match. The part overwritten with null bytes differs for each file.

Upon investigation, we found that the corruption of snapshot user data was caused by a function called “ScopeSnapshots*6,” which was first introduced in Windows 8*7. When this function is enabled, the data to be saved in a snapshot is limited to Windows system-related files, meaning user data will not be saved*8. This function is only applied to the system volume (C drive), but in recent years, many PCs have a drive configuration with just a C drive, so it will have a significant impact.

Details of the functional specifications have not been disclosed, so in part, this is a guess based on the test results, but it appears that the operation limiting the files is not perfectly controlled, and in some cases only part of the user data is saved in the snapshot. It is possible that missing data is overwritten with 0x00 when trying to restore this incomplete user data. Also, resident*9 files were saved to the snapshot when they were user data.

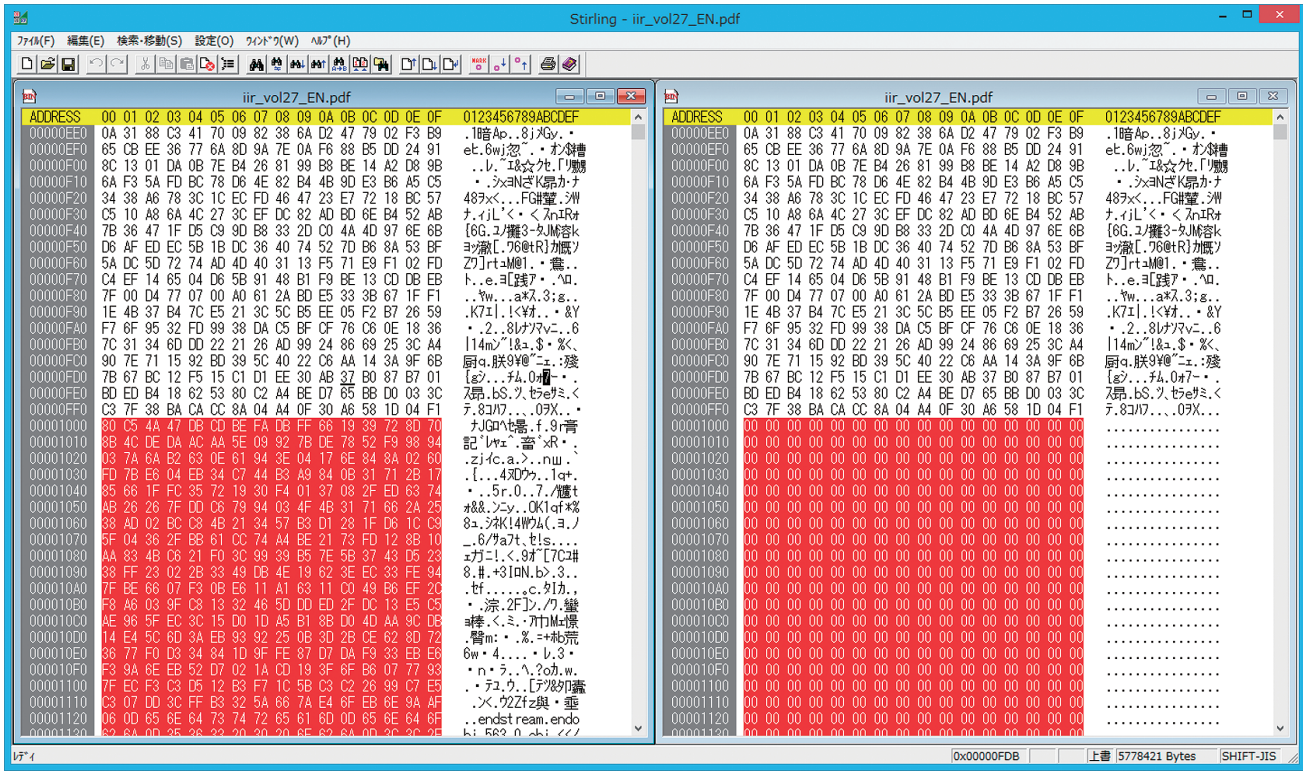

Figure 9: Comparison of Normal and Corrupted Data

*6 Calling SRSetRestorePoint (https://msdn.microsoft.com/en-us/library/windows/desktop/aa378727(v=vs.85).aspx).

*7 We have also received a response from Microsoft indicating that it is highly likely this function is the cause of the file corruption.

*8 Although the reasons for this specification change have not been made public, we speculate that it is related to performance issues from saving all data into a snapshot, utilization efficiency issues in the snapshot area, excessive expansion of user data, and the fact that “file history” is now recommended for backing up user data.

*9 NTFS stores small file data directly in the $DATA attribute of the NTFS MFT record instead of allocating space for it. This state is known as “resident.”

You can disable ScopeSnapshots by creating "ScopeSnapshots" with a DWORD value of "0" in the "HKLM\Software\Microsoft\Windows NT\CurrentVersion\SystemRestore" registry key, and then rebooting the OS (Figure 10). We have also confirmed that it is possible to recover user data from a snapshot correctly in Windows 10 with ScopeSnapshots disabled*10.

As far as we can tell, user data can be recovered correctly from snapshots without disabling ScopeSnapshots in Windows Server products. Table 2 shows whether recovered user data was corrupted in each OS under default settings.

2.7 Conclusion

VSS is a function that has been present since the Windows XP era, but here we identified that the specifications have changed along with updates to the OS version. As such, specifications may change for functions that have been used in the past, so it is important to check for specification updates and verify the tools you use when new OS versions are released.

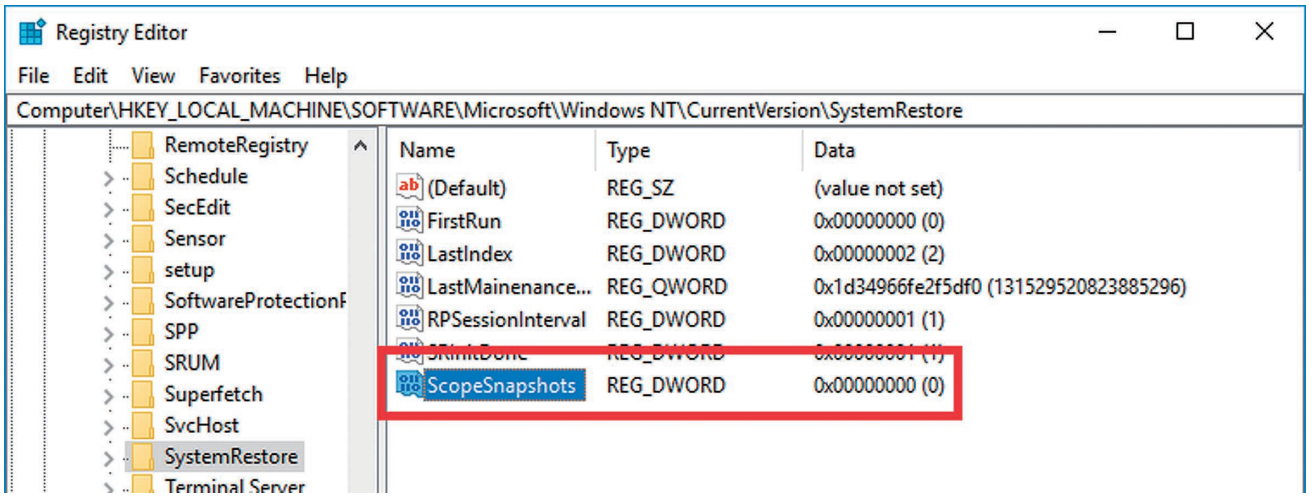

Figure 10: Disabling ScopeSnapshots

Table 2: Corruption of Recovered User Data by OS

	Windows 7 SP1	Windows 8.1	Windows 10	Windows Server 2012/2012 R2	Windows Server 2016
Corruption of Recovered User Data	No	Yes	Yes	No	No

Authors:
Mamoru Saito
Director of the Advanced Security Division, and Manager of the Office of Emergency Response and Clearinghouse for Security Information, IIJ. After working in security services development for enterprise customers, in 2001 Mr. Saito became the representative of the IIJ Group emergency response team IIJ-SECT, which is a member team of FIRST, an international group of CSIRTs. Mr. Saito serves as a steering committee member for several industry groups, including ICT-ISAC Japan, Information Security Operation providers Group Japan, and others.

Minoru Kobayashi (VSS Does Not Protect User Data)
Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, IIJ

*10 We also performed a series of tests using Windows 8.1, and the results were the same as for Windows 10.

The Commercialization and Economic Sphere of Video Over IP Technology

From both a technological and business perspective, we have reached the dawn of a new era in video over IP. Standards for this technology are expected to be published in 2018, and manufacturers are scrambling to comply with these standards. Broadcasters in North America and Europe are also rapidly showing an interest, and sessions featuring this technology have been held at broadcasting equipment exhibitions in Japan. In this report, we will provide details on video over IP technology that many stakeholders have high hopes for.

3.1 Everything is Using IP

It is said to have already been 20 to 30 years since the Internet began to proliferate. Over this period, a variety of media have come to use IP as infrastructure. Media such as newspapers, magazines, and books that used printing technology have embraced the World Wide Web from quite an early stage. The shift of telephone technology from conventional circuit-switching networks to IP infrastructure will also be remembered as a groundbreaking event. That is because this was the moment that telegraph and telephone corporations transformed (or were forced to transform) into telecommunications carriers. Radio is also establishing its presence as an IP-based media through the use of streaming technology. Television broadcasts are actively using IP technology as well. The data broadcasts available through the "d" button on television remote controls adopted streaming technology when they evolved into Hybridcast in 2013. 4K and 8K broadcasts also use an IP format for the broadcast signal itself. As these examples demonstrate, many forms of media have begun to obtain and utilize IP technology.

Among these trends, the latest and most significant involve video and audio signals. Uncompressed audio and video signals (also known as "baseband") that had not been used in streaming technology until now are about to join the IP revolution.

3.2 Baseband and Coaxial Cables

So, where is baseband being used? The main users of baseband are broadcasters and studios. In these kinds of environment, emphasis is placed on obtaining maximum signal quality. For example, broadcasters compress the video signal just before it is converted to broadcast waves. Until this final stage, it is necessary to maintain the highest quality possible for the video signal. This is because image quality will suffer when video with a lot of noise is introduced during the compression process. In other words, the images that television viewers see are originally of a considerably high quality. Coaxial cables have been used as the physical transmission media for video signals in these environments. Looking at a cross section of a coaxial cable, the inner conductor is covered with insulation. Outside of that is the outer conductor, and finally a protective sheathing on the outermost layer. Until now, they have often been used to transmit high-frequency signals, and they are highly resistant to noise. However, due to their characteristics, when you wish to transmit electronic signals in greater numbers or over longer distances, it is necessary to increase the diameter of the coaxial cables to prevent the electronic signal from degrading.

Standards that have been established for the transmission of video using coaxial cables include "SD-SDI" (270 Mb/s, 1990), "HD-SDI" (1.5 Gb/s, 1998), "3G-SDI" (3 Gb/s, 2002), and "6G-SDI" (6 Gb/s, 2015). These standards were created by the SMPTE, and were given the name Serial Digital Interface. 4K broadcasts are implemented at 60 frames per second, so it is not possible to support these using 6G-SDI, which maxes out at 30 frames per second. As a result, a transmission format supporting 4K called "12G-SDI" was established in 2017. It is likely that 12G-SDI will be used for 4K content.

Standard Name	Video Signal (Resolution and Framerate)	Bitrate
HD-SDI	1080i30	1.485 Gbps
3G-SDI	1080p60	2.97 Gbps
6G-SDI	2160p30	6 Gbps
12G-SDI	2160p60	12 Gbps

Table 1: SDI Types and Bandwidth

As it is, a method of transmitting 4K video by bundling four 3G-SDI cables together is presently being used. However, having four coaxial cables bundled together results in a cable that is hard to handle. This is only being used as a stopgap measure, and we expect that migration to 12G-SDI will eventually be necessary.

However, with 12G-SDI there is an issue where cables cannot be lengthened to transmit large amounts of data, so it falls short from a handling perspective. It can only deliver a signal up to about a few dozen meters. Thus, manufacturers focused on optical fiber as the next-generation physical transmission media at the same time as they began developing 12G-SDI. Considering the spread of 4K and 8K going forward, it is clear that coaxial cables will not be able to provide sufficient bandwidth. Because the use of optical fiber is already commonplace in the telecommunications industry, this is a natural choice. When making this selection, Ethernet and IP were chosen as the higher-level protocol for optical fiber. Ethernet and IP technologies are more than widespread enough, and still have room for future development. Instead of creating a proprietary protocol, we will adopt technology that currently exists. This way we will be able to achieve the large-capacity transmissions that optical fiber enables more easily and at an earlier stage.

3.3 Standardization at the SMPTE

In 2017, a standard called “SMPTE ST 2110” became a keyword regarding video over IP. Final publication is scheduled for 2018, and this is expected to be the standard moving forward. Although it has yet to be published, the number of manufacturers planning to support it at the time of release has increased rapidly. This is evidence of how highly anticipated this standard is in the industry.

SMPTE stands for Society of Motion Picture and Television Engineers. The Japanese translation clearly states that it is based in the United States, but the standards it publishes have an impact across the globe. In other words, it serves as a standardization body responsible for global standards.

SMPTE ST 2110 is a standard titled “Professional Media Over Managed IP Networks.” Professional Media refers to technology used at corporations such as broadcasting companies. We also believe that Managed IP Networks refers to closed networks rather than the Internet. ST 2110 is made up of multiple standards, and is called a “protocol suite.” In short, ST 2110 is expected to be a compilation of video over IP standards.

There were examples of technology prior to ST 2110, such as the proprietary video over IP implementations developed by manufacturers. These include Media Global Links’ IP-VRS (IP Video Routing System, 2008 onward), Evertz Microsystems’ Aspen (2013 onward), and Sony’s NMI (Networked Media Interface, 2014 onward), which have all been released to market and put to practical use. Because each of these companies proceeded with development of technology ahead of other companies, they were

Standard Number	Standard Name	Overview and Characteristics
2110-10	System Overview	System timing model & Session Description
2110-20	Uncompressed Video	Based on RFC 4175 32k x 32k, 4:2:2, 4:4:4, HDR (PQ, HLG) etc.
2110-30	PCM Audio	Based on AES67
2110-21	Traffic Shaping	
2110-22	Compressed Video	TBC
2110-31	AES3 Transparent Transport	Includes compressed audio
2110-40	Ancillary Data	Captions, subtitles, time codes, active format description, dynamic range, etc.

Table 2: List of Published SMPTE ST 2110 Standards

forced to create their own standards. These contain functions that have yet to be implemented in ST 2110. However, Evertz has begun promoting support for SMPTE ST 2110, and Sony has given demonstrations and made announcements for gateways and CCUs that support 2110. Manufacturers that led the way will be tasked with finding benefits created through the fusion of their own technology with ST 2110, while manufacturers who enter the market later will need to find a way to market their distinguishing qualities amidst the tidal shift of standardization.

This existence of this prior technology undoubtedly aided the development of 2110. We imagine that the conviction toward and the desire for standardization was generated because technology working on a product level already existed (companies that developed this prior technology most likely wonder what all the fuss is about, although on the other hand, some may feel that this validates their course of action).

When creating the ST 2110 standard, the SMPTE adopted the approach of putting existing standards to effective use. Specifically, they referred to the RFCs of the IETF (Internet Engineering Task Force). Among the standards laid out in these RFCs was a protocol developed for multimedia communications called RTP (Real-time Transport Protocol). RTP has a proven track record in VoIP (Voice over IP), and it can be extended to handle various data payloads (this actually involves drawing up standards for each data format and publishing RFCs). It is also compatible with multicast, and it has been used in many multicast applications. With this history behind it, RTP was the perfect protocol for video over IP.

	Sony IP Live	Evertz Aspen	VSF TR-03 (SMPTE 2110)	VSF TR-04	SMPTE 2022-5/6	IntoPix TICO
Uncompressed Video	NMI	RDD 37 Video PES	RFC 4175	SMPTE 2022-6	Yes	SMPTE 2022-6
Uncompressed Audio	NMI	SMPTE ST 302 Audio PES	AES67 / RFC 3190	AES67 / RFC 3190	Embedded	SMPTE 2022-6
Compressed Video	LLVC	No	No	No	Opt JPEG2K	Yes
Metadata	NMI	SMPTE ST 2038 Meta PES	IETF RTP Proposal	SMPTE 2022-6	Embedded	SMPTE 2022-6
Forward Error Correction	Frame Aligned	No	No	No	Not Aligned	No
Independent Packetization	NMI	TS over SMPTE 2022-2	Yes	No	No	No
Registration and Discovery	Plug & Play (NDCP)	JSON-RPC	AMWA IS-04	AMWA IS-04	No	No
Connection Management	Sony IP Live System Manager	Evertz MAGNUM	AMWA IS-05	AMWA IS-05	No	No
Timing / Sync	SMPTE 2059	TS PCR/PTS	RFC 4566 (SDP)	RFC 4566 (SDP)	No	No
COTS IP Switch	Yes	No	Yes	Yes	Yes	Yes
SMPTE Standard	RDD 34 (LLVC) RDD 40 (NMI) RDD 38 (NDCP) SMPTE 2059 (PTP)	RDD 37 (ASPEN)	VSF Reccomendation (SMPTE 2110 in Process)	VSF Reccomendation	SMPTE 2022-5/6	RDD 35 (TICO)
Interoperability	Guaranteed	Demonstrated	Demonstrated	Demonstrated	Demonstrated	Within TICO Family
Endpoint Validation	Sony Testing Lab	No	No	No	No	No

Table 3: Video Over IP Comparison by Nextera Video*1

*1 Nextera Video, "Video over IP Comparison" (http://www.nexteravideo.com/resources).

Audio shifted to IP technology ahead of video. The CobraNET standard transmits audio data directly over Ethernet frames, and this can be considered the prototype for audio over IP. Then, Dante (Digital Audio Network Through Ethernet) made the leap to using IP. This protocol become popular after it was announced by Audinate in 2006, and it has been adopted in Japan by companies such as Yamaha. However, because this technology is proprietary, a license was required. Following on from this, Ravenna appeared in 2011. Ravenna has the merit of using more standard technology than Dante (Ravenna is the name of the city where Dante, a poet from Florence, met his end). Then, in 2013, AES67 (AES standard for audio applications of networks - High-performance streaming audio-over-IP interoperability) developed by the Audio Engineering Society was published, leading to the standardization of audio over IP. However, a mix of Dante and Ravenna remains in use today.

Multicast is a technology that was published as RFC988 in 1986. IP source address and destination address information is recorded in the header of IP packets. Unique IP addresses are assigned to individual nodes, so it is based on the assumption that communications will be carried out on a one-to-one basis. This communication method is called unicast. On the other hand, multicast implements one-to-many communications for the sender and recipient by applying a concept called “host group” to the IP destination address. This host group is like a television channel or a radio frequency. Put simply, everyone who joins that group can receive the same data simultaneously. For this reason, a special IP address is assigned to the host group.

Multicast is a technology that at one point showed promise for Internet use, and many tests were performed around the world. It was thought to be ideal for broadcast applications. The Rolling Stones live concert footage that was broadcast over multicast in 1994 is now the stuff of legend. IIJ also offered a multicast reception option in its IIJ4U access service.

Video		Audio	Ancillary
2110-20	2110-22	2110-30	2110-40
Uncompressed video	Compressed video	PCM audio	SMPTE ST 291
RFC4175	To be decided	AES67	Awaiting RFC publication
RTP RFC3550			
UDP RFC768			
IPv4 RFC791 (IPv6 RFC8200)			
Ethernet			
Physical Layer			

Figure 1: Relationship Between SMPTE ST 2110 and RFCs in Hierarchical Form

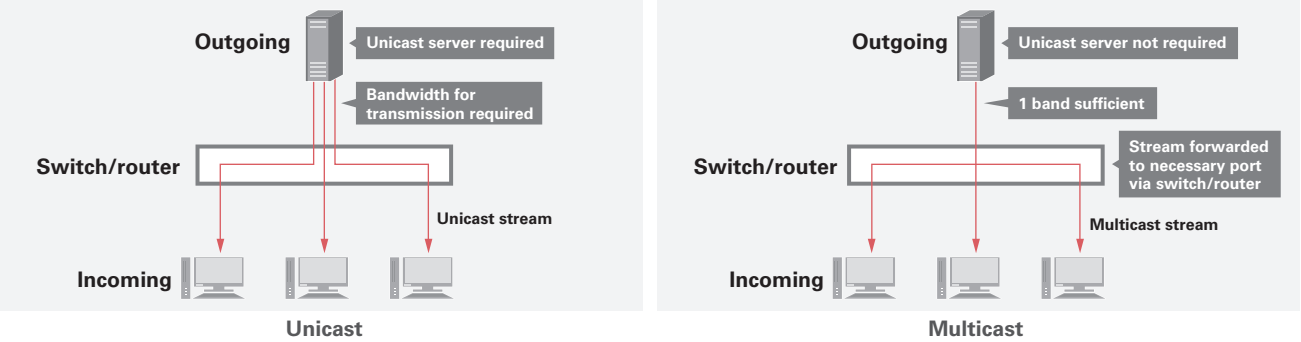

Figure 2: Comparison of Unicast and Multicast

Subsequently, multicast did not see widespread use, as issues such as finding an acceptable method for interconnection on the Internet could not be resolved. However, this technology is still highly effective in closed network environments. The reason for this is that “one-to-many” transmissions are used in broadcast production. Video shot with a single camera is passed on to wherever it is needed. In the world of SDI, there are also devices called routers that are responsible for distributing SDI input electronically and outputting it to designated ports. This flow is just like multicast behavior.

3.4 Trends at International Broadcasting Equipment Exhibitions

NAB Show and IBC are well-known international conventions in the broadcasting industry. The NAB Show is held in Las Vegas every April, attracting an attendance of around 100,000. Meanwhile, IBC is held in Amsterdam each September, and is attended by over 50,000 people. The atmosphere at each show is slightly different, reflecting the state of the U.S. and European broadcasting industries. The largest conventions take place about every six months, and it seems that manufacturers set their development and marketing milestones based on these, such as timing the announcement of new product and feature releases to match convention dates.

Video over IP technology has also attracted significant interest as a next-generation technology at the NAB Show and IBC. An “IP Showcase” where general connection test demonstrations were given for video over IP equipment has been held at successive events, including IBC2016, NAB Show 2017, and IBC2017, attracting industry-wide attention. Over 40 video over IP equipment manufacturers came together to test interconnectivity, and show the audience the connectivity of their equipment.

Figure 3: The IP Showcase at IBC2017

One of the benefits of adopting a standard is interconnectivity. A variety of connections should also be possible. IP and SDI were both originally aimed at achieving this, along with performance, so it assumed that video over IP will also offer this interconnectivity. That said, it is not always that easy to connect successfully. There are gaps in the written standards, and implementation sometimes involves case-by-case judgments, leading to variance in behavior between different manufacturers' equipment.

At these IP Showcases, a hot stage is prepared ahead of the convention, and a system for engineers to perform tests while confined in a "training camp" situation is established. Because it is rare to have the chance to perform tests with multiple manufacturers, it seems that manufacturers consider this a valuable opportunity as well.

3.5 Why Adopt IP?

What exactly are the benefits of IP? "Bidirectionality," "multiplexing," and "interconnection" are some advantages that IP has over SDI. These are all taken for granted with IP, which has been developed on the Internet, but they provide new functionality for broadcasting equipment. When using an optical fiber (one or two cores), there is no longer a need to fix the relationship between the sending and receiving parties. It will also be possible to handle multiple video streams and other media through a single optical fiber. For example, you can consolidate all the filmed images, sound, and its management using IP, such as remote control of audio, intercom systems, and Web-based cameras.

Another advantage of IP is that connections can be made between networks with relative ease. The physical distance between networks is not an issue for these connections. For example, you can set up transmission equipment for each segment to compensate for the degradation of optical fiber, allowing you to leave the problems that must be solved to enable long-distance connections to lower layer technology. As IP is not designed to take distance into account, remote connection can be achieved easily. Of course, the longer the distance, the more time it will take to transmit IP packets, but this issue is not limited to IP.

Also, IP is not only being used as a technology to replace SDI. IP technology is already being used in a variety of areas, such as CDN and OTT, mobile broadcasting out in the field, the migration of FPU to IP, and PC-based editing and station systems. The IP format has even been adopted for electronic wave-based 4K/8K broadcasts. The range of benefits that transition to IP can provide is not limited to switching from a coaxial cable. All station systems and workflows will now operate over IP.

From this perspective, the existence of an ecosystem surrounding IP may be a reason to choose it. The development of IP technology will continue going forward. Even if the SMPTE had come up with a new protocol, the market may not have supported it unless it provided more benefits than IP, or if there were assurances and confidence that it would be widely used.

3.6 A Case Study of IP Applications - Remote Production

Remote production has been proposed as an example of utilizing the benefits of IP. This concept involves broadcasting from a venue in a remote location using an IP network. Currently, broadcasters send a broadcasting vehicle and crew to the venue when creating a program. But when using this method in situations such as the Olympic Games and the Paralympic Games, where events take place at multiple venues simultaneously, there are constraints. Since the number of broadcast vans is limited, you are forced to choose the events to broadcast based on this number.

However, cameras already support remote operation. You can control the direction using a remote camera platform, and remote controls for aperture and focus are also now mainstream. Photographers in the field sometimes only need to be aware of the camera orientation. Other camera functions are controlled by a technician called a video engineer while watching a monitor in the broadcasting vehicle. If this is the case, you might as well connect the video output of the camera to an IP network directly. Then all you need to do is deliver this video via IP to the sub-studio inside the station where the program is being produced. This enables you to minimize the crew that must be physically sent out to venues. As a result, it will be possible for most staff to produce programs while stationed in a sub-studio.

These days, anywhere from two or three cameras to several dozen are set up at a venue for sport broadcasts. Of course, for events where a large number of cameras are required, broadcasting vehicles and crew will continue to be sent to the venue. However, if it is possible to follow the movements of an event with a small number of cameras, and there are no major production issues, we believe remote production will become more meaningful. Of course, you will need to install optical fiber with sufficient bandwidth at the site, but in many cases, this has already been done at major venues. Using this optical fiber to carry Ethernet and IP traffic will create an IP network with ample bandwidth. Broadcasters have also shown a high level of interest in remote production, so PoC tests and implementations are likely to become more prevalent in the future.

3.7 Full-Scale PoC Tests and Proposals

IIJ has carried out PoC (Proof of Concept) tests since 2015 to add momentum to the promotion of video over IP technology. The implementation of 100 GbE on the IIJ backbone is progressing. From a bandwidth perspective, we believed there would be no problem streaming multiple 4K videos. However, there were doubts when we first began working on video over IP technology. We wondered if it would be possible to transmit 4K video that is sensitive to loss and delay over the IIJ backbone, which is comprised of generic IP devices.

Ultimately, the only way to allay these doubts was to try it out. To achieve this, we built a virtual network that would make a

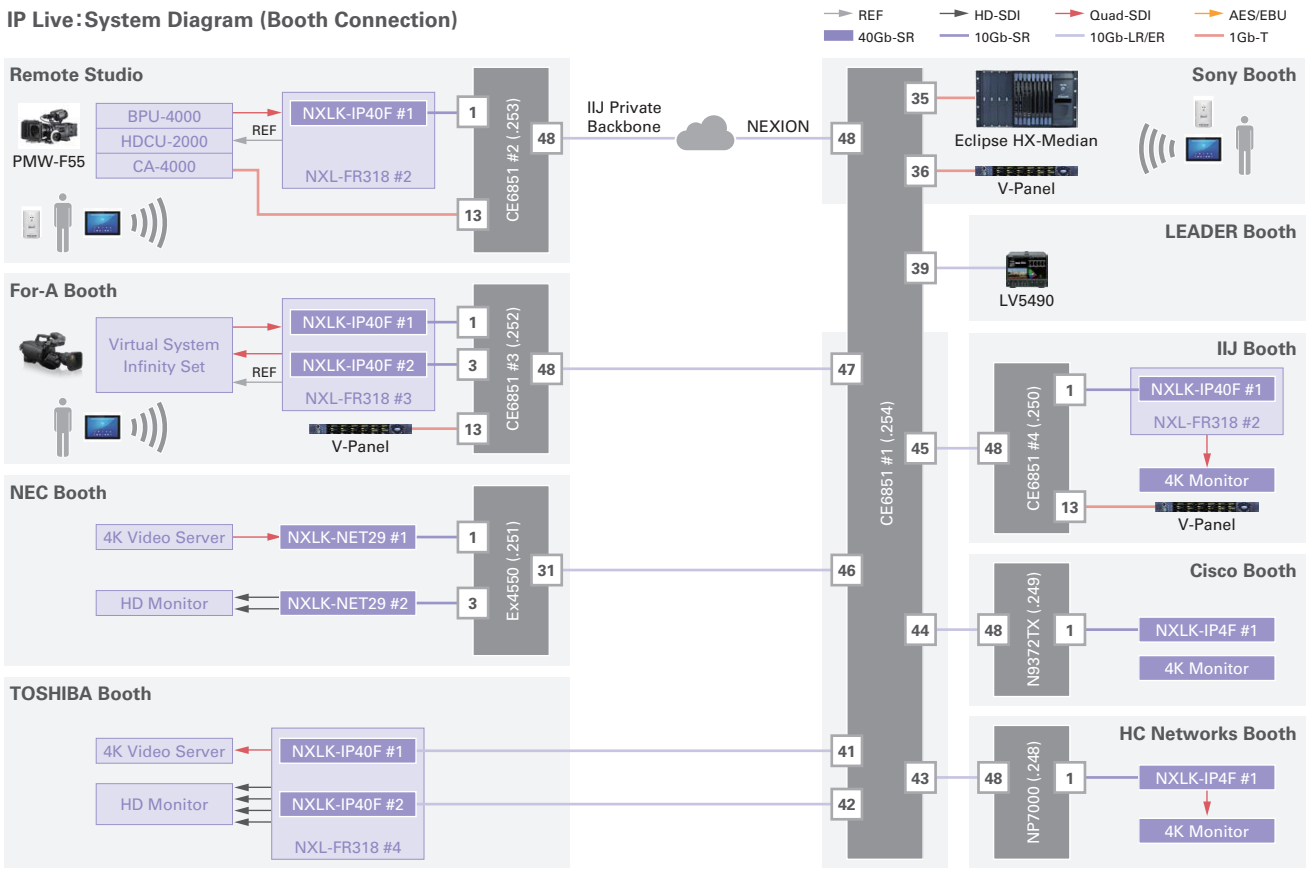

Figure 4: Remote Production Example at Inter BEE 2017
Using the Iidabashi Office of IIJ as a venue (top left of the figure), and connecting the Makuhari Messe Sony booth with the IIJ booth over the network

round trip from our office in Iidabashi, Tokyo, to Osaka. We used our backbone and access optical fiber, along with MPLS routers. Traffic traversing this network is transferred separately from traffic for IIJ's other services, but the dedicated line bandwidth used for lower-level layers is shared. This is because it is costly to construct using only dedicated lines, and IIJ was not interested in performing tests that do not use our actual backbone.

Using this environment, we have continued to perform PoC tests together with manufacturers that have offered to collaborate. The main test involves streaming one or more HD or 4K videos. Some manufacturers are also conducting PTP or audio over IP tests at the same time. Almost without fail, these PoC tests have been successful. When the PoC initiative began at IIJ, few stakeholders had faith in migrating to IP. I remember that users were particularly suspicious of the unfamiliar IP technology. During this period, we promoted the potential of this new technology to these people, but the situation remained unchanged for a while.

At the time, I thought that the shift to IP would come with support for 4K. Using simple calculations, 4K requires eight times the amount of data as HD content (four times the pixels, and double the frame rate). Consequently, when 4K is introduced, the transmission paths of all sections will require eight times the bandwidth. Transmission paths designed and built for HD content do not have enough capacity to transmit 4K signals. I thought that more parties would consider adopting IP technology when designing transmission lines to support 4K. However, HD video over IP is popular in Europe and the United States. This approach is an attempt to enjoy the benefits of IP without waiting for 4K. After asking why, it seems there are many who believe it would lead to cost benefits in the future, and they should start dealing with IP now, without waiting for 4K. This sounds plausible, but when considering the timing of the investment, there remained doubts about whether real benefits could be seen. It may be that there are differences between companies with regard to broadcaster investment. So, as an extreme example, I once saw a presentation where the question "what are the benefits of adopting IP technology?" was answered with a slide that read "because we can." It was most likely some kind of joke, but I felt it was an appropriate response for an engineer.

IIJ aims to build up experience through PoC tests and share this knowledge with manufacturers. This is because we would like to communicate what can be done with IP, while creating an accurate knowledge base and higher-quality know-how. In reality, few manufacturers have experience with tests using wide area networks. We provide manufacturers with data we have obtained through PoC tests, and provide feedback. We are also encouraging end users to observe our PoC projects. Demonstrations using actual networks are very effective, and they are held in high regard for sales and marketing as well.

Period	PoC Test Details
July 2015	Sony IP Live. 4 Gbps x 2 lines transmitted from Iidabashi to Osaka to Iidabashi. Our first video over IP test.
August 2015	Evertz ASPEN. 4K Koshien video transmitted from Grand Front Osaka to Iidabashi.
June 2016	PFU QG70 + NTT-IT StreamMonitor. 1.5 Gbps HD video transmitted from Iidabashi to Interop venue.
October 2016	Sony IP Live. Testing of newly-developed mode. Transmitted from Iidabashi to Osaka to Iidabashi.
November 2016	Sony IP Live. Connection of IIJ booth and Sony booth inside the Inter BEE venue.
February 2017	MediaLinks IP-VRS. Transmission test for HD/4K video. Transmitted from Iidabashi to Osaka to Iidabashi.
June 2017	Sony IP Live. Demonstration incorporating professional video equipment (remote cameras, audio console).
June 2017	Embrionix. HD transmission using SFP video IP conversion. Transmitted from Iidabashi to Osaka to Iidabashi.
June 2017	LAWO V__remote4 + Seiko TS-2950. HD and 4K, 64-channel multi-channel audio transmission. PTP interconnectivity test
November 2017	NHK Science & Technology Research Laboratories. NHK performed 8K transmission tests from Osaka to Tokyo at the 2017 NHK Trophy figure skating. IIJ provided a private backbone for these tests (10 GbE x 5 lines). The 8K footage used Dual Green format at 24 Gbps.

Table 4: Major PoC Tests at IIJ

Proven networking performance for all layers plays an essential role in the success of PoC projects like these. Of course, in addition to network layers, it requires technical knowledge of video and audio. I know from experience gained through many PoC tests that even when the equipment is installed, the necessary settings applied, and all wiring completed, it almost never works the first time. Let us consider why video may not transmit or be played back. There are a variety of possible reasons. These include router or switch configuration errors, bugs, traffic overflow, communication errors, and misunderstandings. Basically, anything could happen. Patiently unravelling these tangled threads one-by-one requires time and effort. We must call upon all the knowledge we possess as engineers, including multicast technology know-how, networking expertise in areas such as IP and Ethernet, and even the physical properties of fiber optic cables. Video often does not play back due to cabling errors. PoC tests are a process of trial and error, so there will inevitably be consideration shortfalls and mistakes. It is necessary to develop the capacity to notice minor points such as these. That said, mistakes and errors that occur during PoC tests are all "gifts" for the future.

3.8 Compression Technology

12G-SDI is necessary for the transmission of uncompressed 4K video. In other words, this requires 12 Gbps of bandwidth, so it is not possible to transmit using a single 10 GbE cable that is commonplace in the Ethernet world. In light of this, calls to shift to 25 GbE have begun to emerge in the broadcasting equipment industry. This will enable uncompressed 4K video to be sent via a single network interface. However, we believe it will be a little longer before for these calls work effectively. That is because it will be some time before Ethernet switches offer 25 GbE support and come down in price.

Uncompressed video is better in terms of latency and image quality, but it requires more bandwidth. Consequently, there have been moves to reduce bandwidth using compression technology. In this area, several compression techniques have already entered the stage.

- JPEG2000: A compression technology that has already been standardized.
- VC-2: Developed by BBC R&D and standardized as SMPTE ST 2042.
- LLVC: Developed by Sony. Stands for Low Latency Video Codec. Reference books have been published as SMPTE RDD 34.
- Tico: Developed by IntoPix. Currently undergoing standardization as JPEG-XS.

Each of these compression technologies are referred to as "visually lossless." They do not offer lossless compression where all data can be retrieved intact after compression. This lossy compression does not allow you to restore the original data completely, but it does not affect the image quality. (So, it is not "lossless" in a strict sense, but this is used as a marketing term.) The fact that the compression does not affect image quality means that subsequent editing work will not be impeded by a deterioration in quality or delays due to compression. It is also called "light compression" in the sense that it "compresses slightly for transmission", as opposed to high compression technology such as HEVC. Another name for it is "mezzanine," because it is the middle ground between uncompressed and highly compressed data. It is mainly aimed at reducing the transmission rate for 4K video to between a half and a quarter.

In some cases, companies have been granted patents for these compression technologies, and it is said that their intentions will affect the standardization process. It is possible that intense discussions will be held regarding various points, such as which technology will be made a standard, and which standards will be mandatory or optional.

3.9 Case Studies and the Future Development of Video Over IP Technology

More and more actual case studies are being presented at the IP Showcases mentioned above. In particular, the shift to adopt IP in the OB Van and OB Truck broadcasting units that are used for outside broadcasting (OB) is making considerable progress. Because the video networks inside these broadcast vehicles are initially closed, it is relatively easy to introduce new technology. The adoption of IP technology in broadcasting vehicles is already gaining momentum in Japan.

A series of major system construction projects were announced in Japan in 2017. Perform Japan adopted Evertz for the DAZN Digital Live Sports Production Center. Sony IP routing equipment was also introduced at Shizuoka Broadcasting and SKY Perfect JSAT in quick succession.

There are also moves to increase the penetration of video over IP technology and draw up a roadmap. The Joint Task Force on Networked Media (JT-NM) is in charge of these efforts. The JT-NM is a joint activity involving the AMWA (Advanced Media Workflow Association), the EBU (European Broadcasting Union), SMPTE, and the VSF (Video Services Forum) that publishes reference architecture and roadmaps. The JT-NM Roadmap of Networked Media Open Interoperability indicates the current status and future development of technology, and it is shared throughout the industry. According to this roadmap, the first phase, "SDI over IP," and the second phase, "Elemental flows," are now almost complete. Up ahead are the third phase, "Auto-provisioning," and the fourth phase, "Dematerialized facilities." Auto-provisioning is aimed at the automation of resource management, and the AMWA has put together a working group and is hammering out standards for this.

As part of the activities of the AMWA, progress is being made with establishing the following three items as NMOS (Networked Media Open Specifications).

- IS-04: Discovery and Registration Specification
- IS-05: Device Connection Management Specification
- IS-06: Network Control Specification

Of these, IS-06 is the most ambitious.

1. Discovery of Network Topology and Discovery of endpoint devices that are connected to the Network Switches
2. Create/Retrieve/Update/Delete Network Streams (Flow Management)
3. Monitoring and Diagnostics

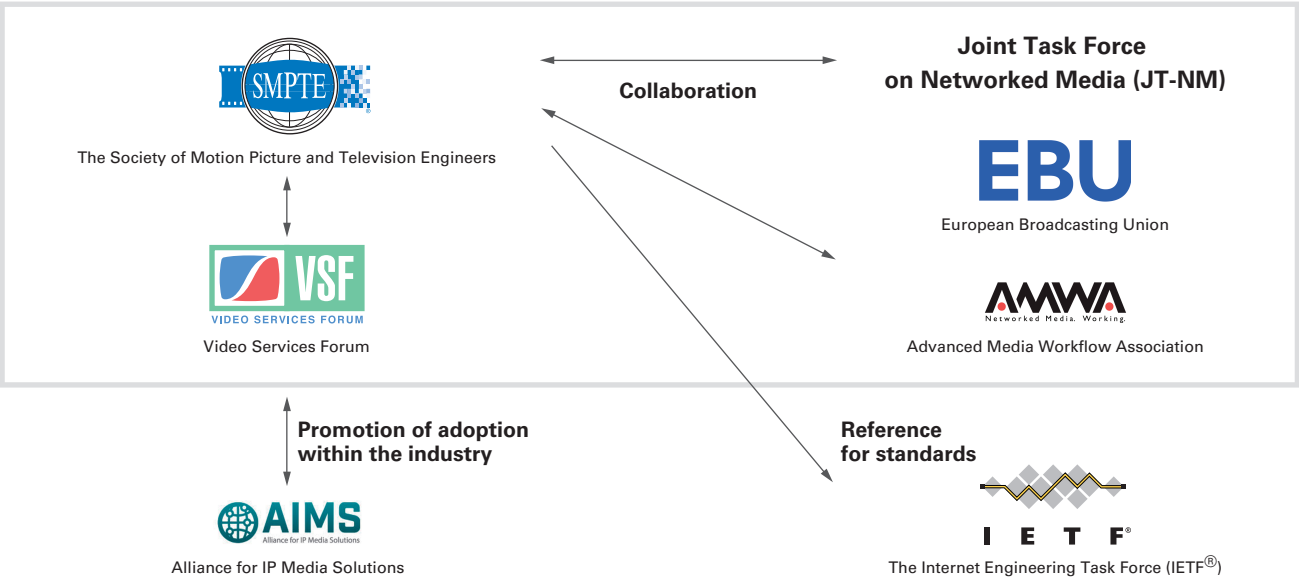

Figure 5: The Relationship Between Standardization Bodies

IS-06 is intended to cover these three functions (they are apparently working on the first of these). This is basically equivalent to the API between the controller and a network device, but you could think of it as an approach similar to SDN. Evertz has also promoted the concept of a Software Designed Video Network in which the network layer is accessed directly from the Application layer via API. The major difference is that IS-06 is attempting to create a standard. Consequently, it is necessary to obtain approval from many network equipment manufacturers. ARISTA has already taken a proactive stance at IBC2017. Support from other manufacturers will no doubt be made clear at some point.

Throughout the activities of the AMWA, there seems to be an increased awareness of security issues. Putting aside the question of which video over IP communities should take part in security-related discussions, there is no doubt that this must be discussed.

Because security covers a wide range of topics, it will be necessary to discuss the areas and perspectives to focus on. Data may still require encryption even when it will be sent over a closed network. In the IP sector, there is a system called IPsec for the generic encryption of IP packets. There is also a standard called Secure Real-time Transport (SRTP) that encrypts RTP, and both have been published as RFC. However, it seems the discussion of which kind of technology to adopt for video over IP has yet to begin.

As for IIJ, the question of how to monetize this video over IP technology is a subject for future analysis. Although we will of course use our backbone, we believe that integration with data centers and cloud solutions will be a major topic. As broadcaster transmissions shift to IP technology through CDN, OTT, Hybridcast, and 4K/8K broadcasts, we will have wide-ranging discussions regarding the benefits that shifting to video over IP will bring.

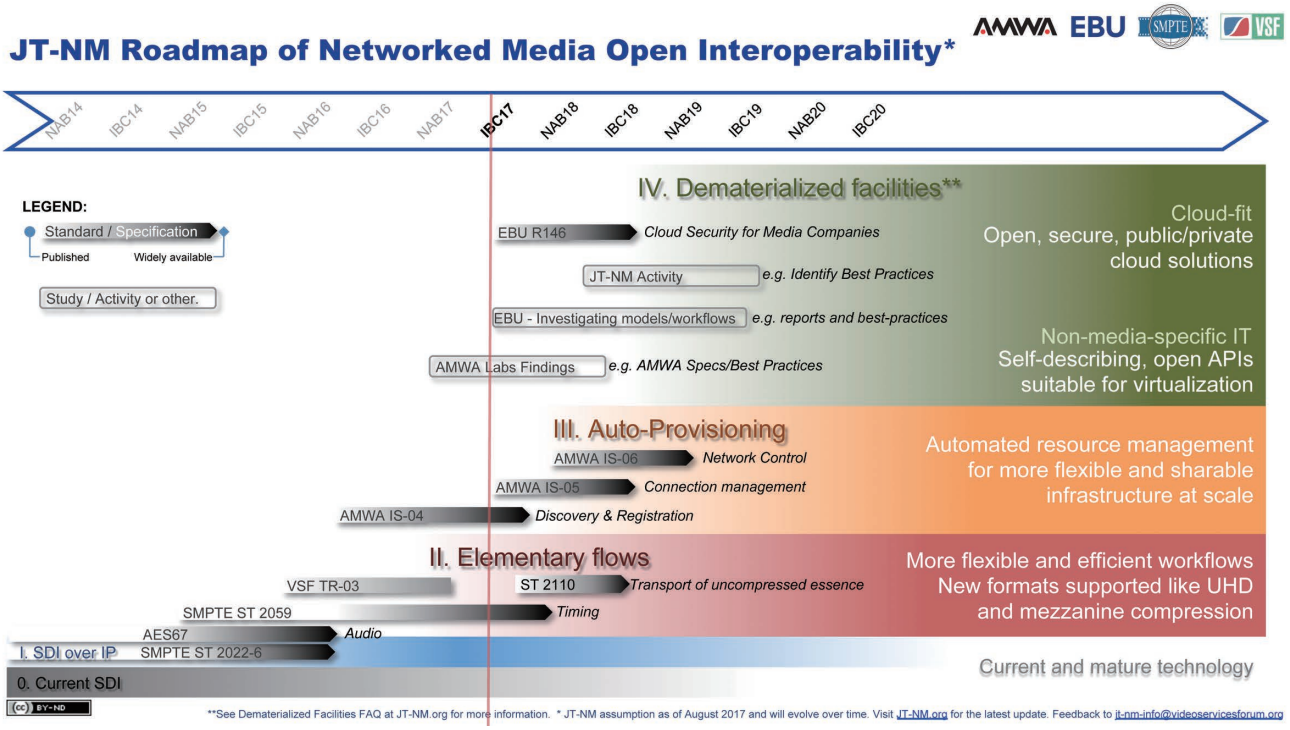

Figure 6: The JT-NM Roadmap of Open Interoperability (August 2017)*2

*2 Joint Task Force on Networked Media (JT-NM) (http://www.jt-nm.org/documents/JT-NM_Networked_Media_Roadmap_of_Open_Interoperability_1708-FINAL.pdf).

Learning about IP technology will be a priority for broadcasters as well. For technology companies in the broadcasting business, IP is already an indispensable technology. Video editing work is transitioning from video tapes to a "file-based" workflow using PC software. Large-capacity storage and workstation PCs are networked to enable the use of non-linear video editing software such as Adobe Premiere and Apple Final Cut Pro. This demonstrates that networks are already an integral part of business, and from an IP perspective video over IP is merely a new application. In any case, it is not possible to comprehend video over IP technology without an understanding of IP technology, so this will become part of an engineer's education going forward.

We must also verify interconnectivity in Japan. IIJ has gained considerable experience through our PoC tests, and I believe this information should be shared widely. This will encourage more people to take part, and we can all work toward a unified goal. As it is not an actual project we can make bold configurations, and try all sorts of things. The best way to achieve this, is establishing a space to verify interconnectivity. With this mindset, IIJ launched an event called "VidMeet." Opportunities to give lectures and demonstrations using video over IP technology in a public place are currently still limited. The video over IP market is now ready to mature, and I believe it is time for people with different needs and wisdom to come together. We intend this to be a place for users, manufacturers, and solution providers to meet, observe field demonstrations, and hold discussions.

The first event, "VidMeet1," was held on October 4, 2017. We gave three lectures and demonstrations to over 100 participants, and received very positive responses. VidMeet2 is set to be held on December 11, 2017, and we look forward to seeing even more people taking part.

Video over IP technology is ripe with the kind of potential you see at the dawn of a new technological era. We are excited to obtain and develop new technology that could revolutionize engineering itself. This is a chance to make new acquaintances in the industry, and discuss topics from a fresh perspective. Times such as these make me thrilled to be an engineer.

Author:
Bunji Yamamoto
Mr. Yamamoto is a Senior Engineer in the Content Delivery and Media Business Department of the Corporate Planning Division, IIJ. He joined IIJ Media Communications in 1995 and has worked at IIJ since 2005. He is mainly involved with the development of streaming technology. Among his contributions to development of the market is the organization of the Streams-JP Mailing List, which discusses this technology.

Intent-Based Network Security

4.1 Introduction

Have you heard of the term “Intent-Based Networking (IBN)”? A certain vendor made a name for themselves by introducing a product line that greatly changes the approach to network design, management, and operation. However, the concept of IBN existed before this, and it does not specify a particular product or solution.

In conventional networks, the intended actions of the user or network administrator are described in the settings for various network equipment. Before configuring network equipment, it is necessary to convert these intended actions into a language that the equipment can interpret, and then can be applied as settings. Regarding the latter, there are multiple methods for reducing the associated load, such as zero-touch provisioning. This enables configuration from a Web-based interface in addition to CLI (command line interface), along with automatic download from networks. However, the network administrator must comprehend the network topology and properties of the equipment to be used before performing the conversion of settings into a language that network equipment can interpret. With mobile and multi-cloud environments often a prerequisite these days, complexity is also increasing.

■ The Focus is “What,” Not “How”

What if the user or network administrator only had to consider “what” they wanted to do, and the network automatically determined “how” to implement the corresponding configuration? On top of that, imagine if the network was able to monitor and manage itself automatically, responding to problems as the situation demanded. IBN is a concept that aims to implement a system that can do both.

4.2 IBN by IIJ

IBN by IIJ is based on the output of research and development for SDN/NFV products that began in earnest at an IIJ group company established in 2012. Figure 1 is a diagram showing the basic architecture of IBN that was built upon this foundation. The user configures “what” action they want to perform on the network via an orchestrator. This input is converted and passed to the controller layer via an Intent North-Bound Interface. The controller can be located on-premises or in the cloud. In addition, a decentralized model is used for the controller layer, with multiple controllers operating in tandem, and the controller layer determining “how” to configure the required settings for network equipment and VNF (Virtual Network Functions) in the network infrastructure layer. VNF can also be located on-premises or in the cloud. Technologies such as OpenFlow or REST API are used as the network controller interface. Our Intent North-Bound Interface is implemented as a proprietary API.

Specifically, with IBN IIJ is aiming to realize a new system of Intent-Based Network Security even with zero trust environments.

■ Zero Trust Environments

As BYOD and IoT have become more popular, a variety of devices are now connected to corporate networks, and it is also common to see places such as medical and manufacturing facilities with a wide range of equipment connected to their network. On the other hand, appropriate security measures are not always applied to these devices. In some cases, devices do not have enough hardware resources to implement security measures, and software embedded in medical or industrial equipment may not be easy to update. Some environments have no supervision over equipment connected to the network. The number

of attacks against specific organizations and people is currently on the rise, and the techniques used are becoming more sophisticated. In other words, no corporate network environment can be considered safe today, which leads to a zero trust approach. Under this philosophy, no user, device, or application is trusted unconditionally. Therefore, verification is always performed to ensure security.

Policy-Based Segmentation

Micro-segmentation is an approach used to minimize the extent of damages when a fault occurs. It can be divided into several categories depending on the target. At IIJ, "policy-based segmentation" is applied based on the two concepts below (policy).

- All users, devices, servers, PCs, and applications are treated equally as "entities" connected to a network
- Entities are only allowed to connect to certain entities

For example, suppose a person belongs to "project a" and "project b". It is possible to apply multiple policies to a single entity, so segments can be assigned for each project. That is to say, a single entity can belong to multiple segments.

This policy-based segmentation is the fundamental idea behind IBN by IIJ. This system only requires you to consider how entities are connected, making it simple and intuitive for network administrators to handle.

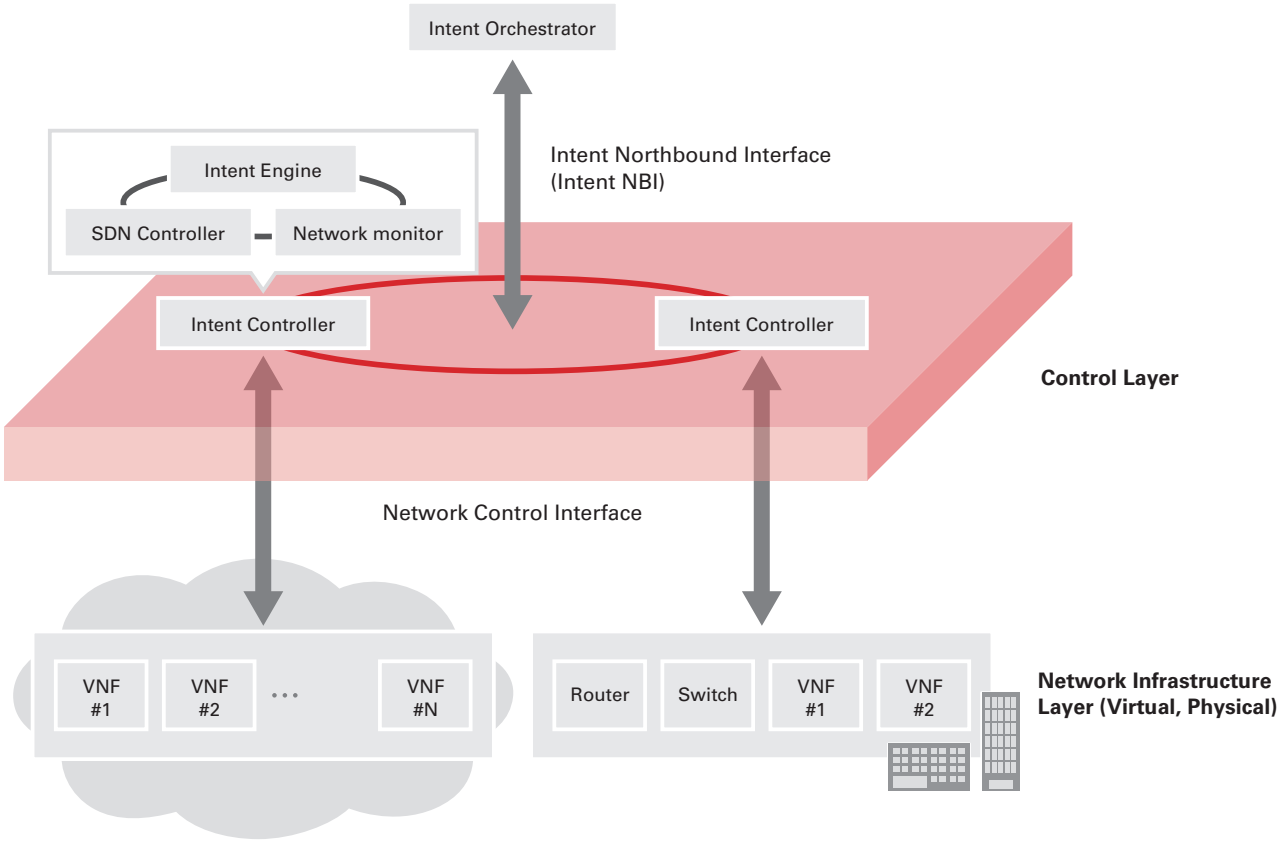

Figure 1: Basic IBN Configuration

Definition of ID and Locator

Normally, an IP address has the dual meaning of ID and locator. While an IP address is a locator (indicating whereabouts) used for routing, from the perspective of upper-layer components such as applications, it is also used as an ID for identifying sessions. As a result, in some cases it is inconvenient for IP addresses to represent two things. For example, when a user or computer moves between networks, a new IP address (both ID and locator) is assigned to the computer, and the session that used the original IP address as the identifier expires. You should only need to update the locator information when a simple change of location is involved, without affecting the ID part of the role.

The main concern of network security administrators is to manage who can access (or cannot access) which information assets, and not the IP addresses themselves. As discussed later, IBN by IIJ solves this issue without managing IP addresses as locators and IDs.

Code Name "FSEG"

Code name "FSEG" is being developed as part of our Intent-Based Network Security initiative. Figure 2 compares the structure of FSEG with the basic structure of the aforementioned IBN. SDN technology is adopted as a method for implementing "monitoring and verification" and "policy-based segmentation" in zero trust environments.

FSEG is an overlay network of which the main components are FSEG controllers and security VNF groups. FSEG controllers can be placed in the cloud, or on PC servers called FSEG nodes in on-premises environments. A full-mesh L3 tunnel connects the FSEG controllers. FSEG controllers have three main functions: authentication of users and devices, policy control (determining the FSEG controllers under which an entity can access devices), and control of security VNF groups (built into FSEG nodes).

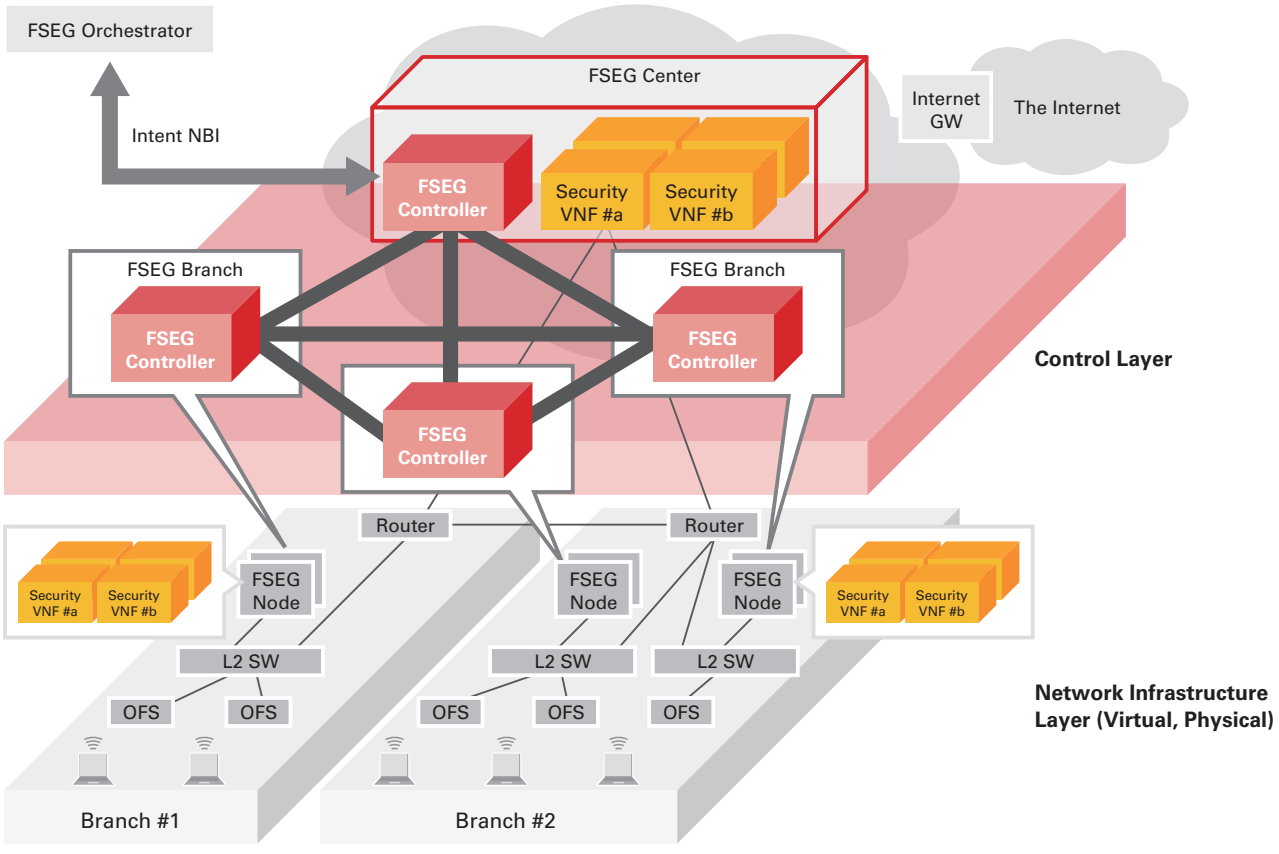

Figure 2: FSEG Overview

FSEG nodes are embedded with security VNF groups in addition to FSEG controllers, and an active-standby configuration for redundancy is an option. Underlay can be simulated with OpenFlow switches connecting users and FSEG nodes in networks.

■ Monitoring and Verification, Segments

Direct communication between devices (port-to-port communication) is prohibited under the OpenFlow switch located within FSEG. All traffic is forwarded to the FSEG node above, so all device-to-device communication is made possible via FSEG nodes. This is for traffic monitoring on FSEG nodes (FSEG controller inside). The FSEG node (FSEG controller inside) also has a policy control function, as well as a database containing policy information indicating "what entity (person or device) can access it." FSEG nodes can apply policies for each type of traffic (controlling the destinations based on the database). Segmentation is implemented by controlling the connection destination for each type of traffic using FSEG nodes. These segments identify "entities," unlike segments based on network equipment settings like conventional VLANs.

The high compatibility with existing networks is one of the characteristics of FSEG. In an FSEG environment, IP addresses are merely underlay technology for connecting entities, and use an FSEG-Private IP address. "Entities" obtain a FSEG-Private address from a DHCP server in FSEG. On the other side, the OpenFlow switches under FSEG nodes can provide NAT function. Therefore, in cases where entities assigned to an existing network use the FSEG environment, this NAT function automatically translates the IP address for inside and outside FSEG. As a result, entities do not need to be aware of changes to the IP address. Regardless of whether the IP address is assigned by the FSEG node DHCP server or the one used in an existing network, the FSEG node manages which type of IP address has been assigned to an entity, so it can be placed under the control of the FSEG controller. FSEG makes it possible to segment all entities and apply policies. This enables existing network environments and FSEG environments to coexist easily, and, for example, customers can start with a small-scale Proof of Concept (PoC).

4.3 Networks with Security Sensors

FSEG Intent-Based Network Security offers new security infrastructure. Not just a concept of intrusion prevention, this constructs a security sensor for early-stage detection and prevention of spreading in enterprise networks today.

■ Entity Authentication

First, FSEG supports multiple authentication systems for a variety of devices to identify entities that are components of policy-based segmentation as below.

- IIJ ID (multi-factor authentication)
- Account + password (Web-based authentication)
- MAC address authentication
- Time range authentication
- Location authentication (which OpenFlow switch it is connected to)
- Combination of the above

Event history is managed for information, such as time range / MAC address / location (switch) / IP addresses, and authentication result.

■ Sharing Threat Information Across All Areas

As mentioned in the previous section, all traffic from entities flows through FSEG nodes, and the FSEG controller on an FSEG node forwards the traffic to associated security VNF. FSEG controllers within the FSEG nodes are also connected via full mesh, and if a threat is detected by a FSEG controller, there is a system for sharing that information with all other FSEG controllers. Each FSEG controller manages whether the security VNF groups under its control are enabled or disabled, as well as which security VNF should be applied to which traffic and in what order (service chaining). Using these systems, after threats are detected in a certain FSEG controller, related FSEG controllers are able to add or edit security VNF, and/or change network settings to isolate the entire segment where the threat was detected. In summary, security sensors covering all networks monitor traffic comprehensively, and can change the shape of networks on the fly based on information obtained through monitoring. Using this same system, load/function balancing between on-premises and cloud can be implemented. For example, when an IPS function located on-premises fails to keep up with processing, a new IPS function can be set up in the cloud to implement load balancing.

■ Preventing Infection

A policy-based segment is a set of entities to which the same policy can be applied. If you were to compare it to a company, it would resemble a group of users and devices in the same department that connect to the same internal work server. A threat discovered in a department could have already spread throughout the department by the time it is discovered. When using FSEG, you can prevent infection in a segment by changing the policy of the segment to which it belongs, based on the threat information found by security sensors. This enables you to perform settings to prevent infection dynamically, such as changing the level of traffic monitoring for each segment where threats are found, or applying new security VNF, to minimize any unexpected damage.

■ Placing Security on Networks

As previously mentioned, we should not assume that security functions have been applied to IoT devices themselves. With government work style reform, in the near future many IoT devices will be used in offices to make the work environment more convenient. These will not operate independently, as communications will always occur with entities outside the device as well. We need to implement security functions on the network side to detect and remove threats. FSEG is the best solution for IoT environments as well, as it treats everything as an entity, while also providing security and preventing infection throughout the entire network.

4.4 Outlook for FSEG

The IBN by IIJ initiative has two strengths. First, we began research and development for SDN technology products at an early stage, and our work is based on the achievements and know-how that we built up by providing our own SDN solutions ahead of other companies, particularly in the enterprise domain. For example, we utilize it to manage traffic used for policy-based segments as described in this report. Our other strength is that we defined a clear and specific use-case, namely providing a new security system for enterprise networks. As a result, it has been easier to obtain the cooperation of partner companies, implementation has already been performed using the methods described here, and a PoC has also been completed.

■ CPE and Switches

While considering the use-case, you should think about how you will provide the service. When providing FSEG as an IIJ solution, we must consider how to design and implement FSEG nodes as CPE installed on the customer side. As mentioned above, in FSEG operation all traffic flows through FSEG nodes. This means traffic loads are concentrated on the FSEG nodes. We have dispelled these concerns using the following three approaches. First, we built a system that did not always require traffic to pass over FSEG

nodes. In cooperation with the OpenFlow switch under an FSEG node, a decision is made for each flow about whether to pass traffic through FSEG nodes. Secondly, the FSEG node itself automatically scales out under high loads. Finally, we use technologies such as DPDK and ASIC for hardware acceleration. We will combine these in the future, so that we can prepare the most suitable solutions for our customers.

Also, although we described a configuration featuring OpenFlow switches under FSEG nodes, OpenFlow switches are not necessarily required. In such cases, entities are directly connected to FSEG nodes, and the functions of the OpenFlow switch explained here (such as prohibiting direct communication between entities) are implemented on the FSEG nodes.

■ Linking to SOC

What is needed to further enhance FSEG implementations of Intent-Based Network Security? FSEG, a security sensor that encompasses an entire network, can collect data from sensors. It is also able to convert "what" the desired action is into "how" it will be implemented. What is missing is a function for determining "what" to do based on large quantities of data. In other words, the goal is "utilizing a large amount of collected data and knowledge-based analysis." IIJ has also launched the wizSafe security brand as part of our security initiatives. The Security Operation Center (SOC) is also up and running, analyzing vast quantities of data and accumulating knowledge. We are considering linking these with FSEG to build a more robust and sophisticated security infrastructure.

■ Conclusion

The approach of customers only needing to be aware of "what" they want to achieve, leaving the question of "how" to implement this up to IIJ, is something that we have been working on for a while. In this report, we discussed our FSEG solutions, which are part of our IBN initiative based on SDN and NFV technology. However, earlier technologies that IIJ developed such as SMF*1, SACM*2, and Omnibus*3 have also brought this concept to fruition. We will continue to develop FSEG, carrying the torch forward and striving to incorporate cutting-edge technology.

Author:
Masakazu Mizuno
Mr. Mizuno is a Senior Product Manager in the SDN Development Department of the Network Division, IIJ. He has been engaged in the development of products and business with SDN/NFV technology since Stratosphere Inc.

*1 SMF (SEIL Management Framework): patented in March, 2006 (patent 3774433).
*2 SACM (Service Adaptor Control Manager): management service infrastructure for providing auto-connect and comprehensive management systems for SMFv2 (Japan: patent 4463868, United States: patent 7660266) to OEM. SMFv2 enables the centralized management of not only "SEIL series" products but also the network equipment of other companies, covering everything from initial settings to configuration changes and operation management.
*3 Omnibus: a new cloud-based network service that utilizes SDN and NFV technology (https://www.iij.ad.jp/omnibus/) (in Japanese).

December 2017 Vol.37

IIJ
Internet Initiative Japan

About Internet Initiative Japan Inc. (IIJ)

IIJ was established in 1992, mainly by a group of engineers who had been involved in research and development activities related to the Internet, under the concept of promoting the widespread use of the Internet in Japan.

IIJ currently operates one of the largest Internet backbones in Japan, manages Internet infrastructures, and provides comprehensive high-quality system environments (including Internet access, systems integration, and outsourcing services, etc.) to high-end business users including the government and other public offices and financial institutions.

In addition, IIJ actively shares knowledge accumulated through service development and Internet backbone operation, and is making efforts to expand the Internet used as a social infrastructure.

IIJ-MKTGIIJ-MKTG020-0035

Internet Initiative Japan Inc.

Address: Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku,
Tokyo 102-0071, Japan
Email: info@iij.ad.jp URL: https://www.iij.ad.jp/en/